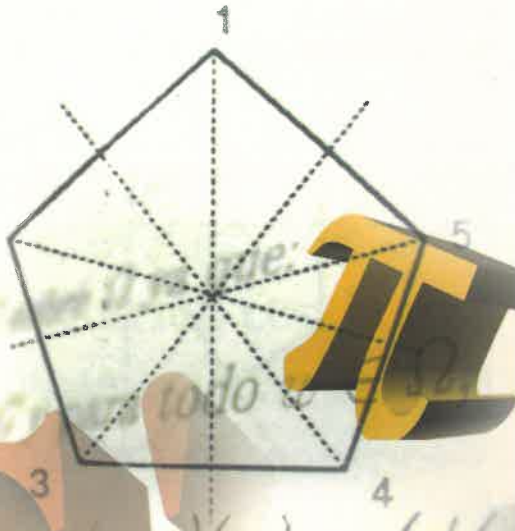
Teoría de Grupos

Mª Angeles Moreno Frías
Enrique Pardo Espino



textos básicos UNIVERSITARIOS 14

SERVICIO DE PUBLICACIONES UNIVERSIDAD DE CÁDIZ

Teoría de Grupos

Mª Ángeles Moreno Frías
Enrique Pardo Espino

UCA Universidad de Cádiz

Servicio de Publicaciones
2003

Moreno Frías, María de los Ángeles

Teoría de grupos / Mª Ángeles Moreno Frías, Enrique Pardo Espino. -- Cádiz : Universidad, Servicio de Publicaciones, 2002. -- 192 p.

ISBN 84-7786-807-7

1. Grupos, Teoría de. I. Pardo Espino, Enrique. II. Universidad de Cádiz. Servicio de Publicaciones, ed. II. Título.

51

Edita: Servicio de Publicaciones de la Universidad de Cádiz

Depósito legal: CA-882/02
I.S.B.N.: 84-7786-807-7

Diseño: Cadigrafía
Maquetación y fotomecánica: Produce
Imprime: Santa Teresa

Índice general

Prólogo

Este libro está pensado como un manual con el que los alumnos de Matemáticas españoles (y especialmente los gaditanos) puedan adentrarse en los aspectos más fundamentales de este tema, a través de una exposición organizada y detallada del mismo. No pretende ser el manual definitivo para la enseñanza de la Teoría de Grupos, ni mucho menos sustituir las extraordinarias y completas monografías sobre el tema, que especialistas como Rotman, Suzuki o Kurosh pusieron al alcance de la comunidad científica.

Es el resultado de la experiencia de ambos autores, que han impartido ésta y otras asignaturas de similar contenido; ello se refleja en determinadas maneras de introducir ciertos temas y resultados, o de considerar los detalles y comentarios a las demostraciones. Es en esto en lo que se puede diferenciar de las antes mencionadas monografías: pretende ser cercano y fácilmente comprensible para no especialistas. Tampoco pretendemos ser absolutamente originales, y por tanto el texto se ha alimentado de diversas fuentes bibliográficas, que se reseñan al final del libro.

El texto se divide en siete capítulos. El esquema escogido se corresponde con el programa de la asignatura "Teoría de Grupos", que se imparte durante un cuatrimestre y que es obligatoria para los alumnos del primer ciclo de la Licenciatura de Matemáticas de la Universidad de Cádiz. El programa cubre, por este orden, los siguientes aspectos básicos:

1. Grupos, subgrupos y grupos cociente.
2. Morfismos de grupos, y Teoremas de Isomorfía.
3. Grupos abelianos finitamente generados.
4. Grupos de permutaciones.
5. Teoremas de Sylow.
6. Series de grupos.
7. Grupos libres, y presentaciones de grupos.

Los dos primeros capítulos se dedican a introducir y estudiar los elementos básicos de la teoría: objetos y aplicaciones entre ellos. El Capítulo 3 estudia los grupos abelianos finitamente generados, que constituyen una de las dos clases de grupos básicas más importantes. Este estudio se hace utilizando técnicas propias del Álgebra Lineal, lo que en principio facilita al alumno su aproximación al tema. El Capítulo 4 abarca la otra clase básica fundamental de grupos: los grupos de permutaciones. Aplicamos este estudio para el cálculo del grupo de simetrías de un polígono regular de n lados. En el Capítulo 5 se presentan técnicas de acciones de grupos sobre conjuntos, y en él se estudian los Teoremas de Sylow, que nos van a permitir conocer algunas propiedades de un grupo finito en función de su cardinalidad; cabe destacar que la demostración de los mismos que presentamos es poco habitual, y hace mucho hincapié en el uso de diversas acciones de grupos sobre conjuntos, a diferencia de la mayor parte de los textos. El Capítulo 6 abarca los fundamentos sobre el uso de series normales para estudiar grupos, y pone en contacto al alumno, por primera vez, con las técnicas fundamentales para el desarrollo del trabajo de Abel sobre resolubilidad de ecuaciones polinomiales, que se estudia en cursos posteriores. El Capítulo 7 proporciona las herramientas básicas para el trabajo de grupos dados por generadores y relaciones, instrumento fundamental para la Topología Algebraica.

Cada capítulo viene acompañado de una lista de ejercicios, que consideramos adecuados para mejorar la comprensión, por parte del estudiante, de los conceptos desarrollados. El objetivo no es que sea exhaustiva, sino que obligue al estudiante a reflexionar sobre los aspectos de la materia.

Para finalizar, los autores quisieran agradecer a sus familias la paciencia y los ánimos constantes y al Departamento de Matemáticas de la UCA, del que son miembros, el apoyo proporcionado para llevar a cabo la empresa; especialmente a las profesoras Dña. Concepción García Vázquez, por ayudarnos en la realización de los dibujos que ilustran el Capítulo 4 y a Dña. Alicia Cornejo Barrios por su ayuda en la maquetación de la versión final del trabajo.

Puerto Real (Cádiz), Marzo de 2002.

Los autores.

Capítulo 1

Grupos y Subgrupos

El objetivo de este capítulo es presentar los objetos a estudiar, así como sus propiedades básicas. Haremos especial hincapié en las propiedades asociadas a la cardinalidad del grupo y de sus generadores.

1.1. Definiciones. Primeras propiedades

En primer lugar, procedemos a introducir la noción básica fundamental del curso.

Definición 1.1.1 *Un grupo es un par $(G, \cdot)$, donde G es un conjunto no vacío y $\cdot$ es una ley de composición interna definida en G,*

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (x, y) & \longrightarrow & x \cdot y \end{array}$$

tal que verifica las siguientes propiedades:

1. *Asociativa:* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall\, x, y, z \in G$.
2. *Existencia de elemento neutro: Existe* $e \in G$ *tal que* $x \cdot e = e \cdot x = x$, $\forall\, x \in G$.
3. *Existencia de elemento simétrico: Para cada* $x \in G$, *existe* $x' \in G$ *tal que* $x \cdot x' = x' \cdot x = e$.

Cuando no exista riesgo de confusión con la operación interna que estemos utilizando, diremos simplemente que G es un grupo. Asimismo, escribiremos ab en vez de $a \cdot b$.

Definición 1.1.2 *Si en un grupo G se verifica la propiedad conmutativa, es decir $xy = yx$ para todo $x, y \in G$, diremos que G es un grupo conmutativo o abeliano.*

Si G es un grupo conmutativo, denotaremos la operación con el símbolo $+$.

Lema 1.1.3 *Sea G un grupo, entonces se verifica:*

1. *El elemento neutro e del grupo G es único.*
2. *Para cada $x \in G$, existe un único simétrico $x' \in G$.*

DEMOSTRACIÓN.

1. Supongamos que e_1, e_2 sean elementos neutros en G. Entonces se verifica
$$e_1 = e_1 e_2 = e_2.$$
2. Supongamos que x' y x'' sean elementos simétricos de x en G. Entonces se verifica
$$x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''.$$

■

Notación 1.1.4 *En lo que sigue y siempre que no exista riesgo de confusión, el elemento neutro de G, que hemos demostrado que es único, lo denotaremos por 1 y al elemento simétrico de $x \in G$, que también hemos demostrado que es único, lo denotaremos por x^{-1}. Asimismo, si G es abeliano, denotaremos por 0 al elemento neutro, y para cada $x \in G$, denotaremos por $-x$ al simétrico de x.*

Lema 1.1.5 *Sea G un grupo, entonces se verifica:*

1. $(xy)^{-1} = y^{-1}x^{-1}, \qquad \forall x, y \in G.$
2. $(x^{-1})^{-1} = x, \qquad \forall x \in G.$
3. $(1)^{-1} = 1.$

DEMOSTRACIÓN.

1. $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1.$
De igual forma se demuestra que $(y^{-1}x^{-1})(xy) = 1$. Entonces, al ser único el simétrico de un elemento, tendremos que
$$(xy)^{-1} = y^{-1}x^{-1}.$$
2. Como $x^{-1}x = xx^{-1} = 1$, entonces podemos afirmar que
$$(x^{-1})^{-1} = x.$$

3. Como $1 \cdot 1 = 1$, tendremos que $1^{-1} = 1$.

■

A continuación vamos a demostrar que en un grupo siempre es posible simplificar, es decir toda ecuación lineal tiene una única solución.

Corolario 1.1.6 *Sea G un grupo y a, b, c elementos de G, entonces se verifica:*

1. *Si $ab = ac$, entonces $b = c$.*

2. *Si $ba = ca$, entonces $b = c$.*

DEMOSTRACIÓN.

1. Sea $ab = ac$. Como en un grupo todo elemento tiene simétrico entonces podemos asegurar que existe $a^{-1} \in G$. Por tanto podemos efectuar la siguiente operación:
$$a^{-1}(ab) = a^{-1}(ac).$$
Así $(a^{-1}a)b = (a^{-1}a)c$, es decir $1b = 1c$, o lo que es lo mismo $b = c$.

2. Se demuestra de manera análoga.

■

Vamos a ver a continuación algunos ejemplos de grupos.

Ejemplos 1.1.7 *1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$ son grupos abelianos, cuyo elemento neutro es el número cero y el simétrico es el opuesto del número dado.*

2. $(\mathbb{Z}, \cdot)$ no es un grupo, ya que el número $5 \in \mathbb{Z}$ no tiene inverso en $\mathbb{Z}$.

3. Sean $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Entonces se verifica que $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ son grupos abelianos, donde $\cdot$ representa el producto usual. El elemento neutro es el número 1 y el simétrico es el inverso del número dado.

4. El conjunto $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ es un grupo con la multiplicación compleja. Para verlo describimos el conjunto S^1 como
$$S^1 = \left\{\exp^{2\pi i\theta} : \theta \in [0, 1)\right\},$$
donde $\exp^{2\pi i\theta} \exp^{2\pi i\beta} = \exp^{2\pi i\gamma}$ con $\gamma \equiv \alpha + \beta (mód \mathbb{Z})$.

5. *Sea $GL_n(\mathbb{R})$ el conjunto formado por las matrices cuadradas de orden n con coeficientes en $\mathbb{R}$ cuyo determinante es no nulo, es decir,*

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}.$$

Entonces se verifica que $(GL_n(\mathbb{R}), \cdot)$ es un grupo, donde $\cdot$ representa a la multiplicación usual de matrices. Observemos que, si $n \geq 2$, $(GL_n(\mathbb{R}), \cdot)$ es un grupo no abeliano, ya que

$$\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}.$$

6. *Asimismo*

$$O_n(\mathbb{R}) = \left\{A \in M_n(\mathbb{R}) : A^{-1} = A^t\right\},$$

es un grupo no abeliano respecto la multiplicación usual de matrices.

7. *Sea X un conjunto no vacío. Denotaremos por $Biy(X)$ el conjunto de las aplicaciones biyectivas definidas en X, es decir*

$$Biy(X) = \{f : f \text{ es aplicación biyectiva en } X\}.$$

Entonces $(Biy(X), \circ)$, donde $\circ$ representa la composición de aplicaciones, es un grupo. Para verlo definimos la siguiente operación en $Biy(X)$:

$$\begin{array}{rcl} Biy(X) \times Biy(X) & \xrightarrow{\circ} & Biy(X) \\ (f, g) & \longrightarrow & f \circ g. \end{array}$$

Se verifica:

a) *$\circ$ es operación interna, ya que la composición de dos aplicaciones biyectivas definidas en X, sigue siendo una aplicación biyectiva en X, luego*

$$\forall\, f, g \in Biy(X), \text{ se tiene que } f \circ g \in Biy(X).$$

b) *Propiedad Asociativa: Para todo $f, g, h \in Biy(X)$ se tiene que*

$$(f \circ g) \circ h = f \circ (g \circ h),$$

ya que la composición de aplicaciones verifica la propiedad asociativa.

c) *Existencia de elemento neutro: El elemento neutro es la aplicación identidad Id_X, que es una aplicación biyectiva definida por:*

$$\begin{array}{rcl} Id_X : X & \longrightarrow & X \\ x & \longmapsto & x. \end{array}$$

d) *Existencia de elemento simétrico: Para toda aplicación $f \in Biy(X)$ sabemos que existe $f^{-1} \in Biy(X)$ tal que verifica*

$$f^{-1} \circ f = f \circ f^{-1} = Id_X.$$

Así concluimos que $(Biy(X), \circ)$ es un grupo. También se le suele denotar por $S(X)$, en cuyo caso se le denomina grupo de permutaciones del conjunto X. En el caso que X sea el conjunto finito $E_n = \{1, 2, \ldots, n\}$, se denota a $S(E_n)$ por S_n. Este grupo tiene un interés relevante, y dedicaremos a su estudio el Capítulo 4.

Observemos que para $n \geq 3$, $(S_n, \circ)$ no es abeliano. En efecto, sea el conjunto $X = \{1, 2, 3\}$ y consideremos las aplicaciones $f, g \in S_3$ definidas por

$$\begin{cases} f(1) = 2 \\ f(2) = 3 \\ f(3) = 1 \end{cases} \qquad \begin{cases} g(1) = 2 \\ g(2) = 1 \\ g(3) = 3. \end{cases}$$

Se tiene que $(g \circ f)(3) = 2$ y $(f \circ g)(3) = 1$, por tanto $g \circ f \neq f \circ g$.

Definición 1.1.8 *Si G es un grupo y $m \in \mathbb{Z}$, definimos las potencias enteras de un elemento $a \in G$ como sigue:*

$$a^m = \begin{cases} \overbrace{a \cdots a}^{(m)} & si \quad m > 0 \\ 1 & si \quad m = 0 \\ \overbrace{a^{-1} \cdots a^{-1}}^{(-m)} & si \quad m < 0. \end{cases}$$

En el caso de un grupo abeliano $(G, +)$, si $m > 0$, tenemos $a^m = \overbrace{a + \cdots + a}^{(m)} = ma$.

De la definición se desprende el siguiente resultado, cuya demostración es inmediata.

Proposición 1.1.9 *Sean G un grupo, $a \in G$ y $m, n \in \mathbb{Z}$. Entonces se verifica:*

1. $a^m a^n = a^{m+n}$.
2. $(a^m)^n = a^{mn}$.

Proposición 1.1.10 *Sean G_1 y G_2 dos grupos. Definimos en el conjunto $G_1 \times G_2$ la operación $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$. Entonces se verifica que $(G_1 \times G_2, \cdot)$ es un grupo.*

DEMOSTRACIÓN. Veamos que se verifican las condiciones necesarias para ser grupo

1. La operación $\cdot$ es una operación interna, ya que para todo (a_1, a_2), $(b_1, b_2) \in G_1 \times G_2$, se tiene que $a_1, b_1 \in G_1$ y $a_2, b_2 \in G_2$. Por tanto $a_1 b_1 \in G_1$ y $a_2 b_2 \in G_2$. De ahí que
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) \in G_1 \times G_2.$$

2. La propiedad asociativa en $G_1 \times G_2$ es consecuencia inmediata de la asociatividad en G_1 y G_2.

3. Existencia de elemento neutro. El elemento $(1, 1)$ es el elemento neutro, ya que para todo $(a_1, a_2) \in G_1 \times G_2$, se tiene que
$$(a_1, a_2) \cdot (1, 1) = (1, 1) \cdot (a_1, a_2) = (a_1, a_2).$$

4. Existencia de elemento simétrico. Dado un elemento $(a_1, a_2) \in G_1 \times G_2$, se tiene que
$$(a_1, a_2) \cdot (a_1^{-1}, a_2^{-1}) = (1, 1) = (a_1^{-1}, a_2^{-1}) \cdot (a_1, a_2).$$
Por tanto el elemento $(a_1^{-1}, a_2^{-1}) \in G_1 \times G_2$ es el elemento simétrico de (a_1, a_2).

■

A este grupo se le denomina el producto directo de G_1 y G_2. A continuación vamos a ver las condiciones necesarias y suficientes para que $G_1 \times G_2$ sea un grupo abeliano.

Proposición 1.1.11 *Consideremos los grupos G_1 y G_2. Entonces son equivalentes:*

1. *$G_1 \times G_2$ es abeliano.*
2. *G_1 y G_2 son grupos abelianos.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2) : Veamos que G_1 es un grupo abeliano. Sean $a, b \in G_1$. Como $G_1 \times G_2$ es abeliano, se tiene
$$(ab, 1 \cdot 1) = (a, 1) \cdot (b, 1) = (b, 1) \cdot (a, 1) = (ba, 1 \cdot 1),$$
y de ahí que $ab = ba$ para todo $a, b \in G_1$. De igual forma se demuestra que G_2 es un grupo abeliano.

(2) $\Longrightarrow$ (1) : Dados (a_1, a_2), $(b_1, b_2) \in G_1 \times G_2$, se tiene que
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2) = (b_1, b_2)(a_1, a_2),$$
ya que G_1 y G_2 son abelianos. Así, $G_1 \times G_2$ es un grupo abeliano.

■

Definición 1.1.12 *En general, dados los grupos $G_1, \ldots, G_n$, definimos por recurrencia el producto directo de la familia $\{G_i\}_{i=1}^n$,*

$$G_1 \times G_2 \times \cdots \times G_n = (G_1 \times G_2 \times \cdots \times G_{n-1}) \times G_n.$$

Se dice que $G_1 \times G_2 \times \cdots \times G_n$ es el producto directo de los grupos $G_1, G_2, \ldots, G_n$.

Observación 1.1.13 *La definición de producto directo de una familia finita de grupos extiende de manera natural a una familia arbitraria.*

1.2. Subgrupos. Subgrupo generado por un conjunto

La noción de subobjeto reviste, en Álgebra moderna, un valor esencial, por la preservación de propiedades en subconjuntos, es decir, por restricción de problemas elementales a partes más simples.

Definición 1.2.1 *Dados $(G, \cdot)$ un grupo y H un subconjunto no vacío de G, diremos que H es un subgrupo de G si H es un grupo respecto de la misma operación que dota a G de estructura de grupo.*

Proposición 1.2.2 *Dados $(G, \cdot)$ un grupo y H un subconjunto no vacío de G, entonces H es subgrupo de G si y sólo si:*

1. *Para cualesquiera $x, y \in H$ se tiene $xy \in H$.*
2. *$1 \in H$.*
3. *Para todo $x \in H$ se tiene $x^{-1} \in H$.*

DEMOSTRACIÓN.
$\Longleftarrow$: Es inmediato, ya que basta observar que la condición (1) nos dice que la operación $\cdot$ es interna en H, la condición (2) afirma que 1 es el elemento neutro de H, y la condición (3) dice que todo elemento de H tiene inverso perteneciente también a H. Por tanto, sólo nos falta ver que se verifica la propiedad asociativa. Pero si $x, y, z \in H$, entonces $x, y, z \in G$ y por tanto,

$$x(yz) = (xy)z.$$

$\Longrightarrow$: Si H es subgrupo de $(G, \cdot)$, tenemos que $(H, \cdot)$ es un grupo, por tanto se verifica:

(1) La operación $\cdot$ es interna en H y así para cualquier par de elementos $x, y \in H$ se tiene que $xy \in H$.

(2) Sea 1_H el elemento neutro en H, por tanto para todo $x \in H$ se tiene

$$x1_H = 1_H x = x.$$

Pero por otra parte, como $x \in G$, también se tiene

$$x1 = 1x = x.$$

Por tanto, para todo $x \in H$ se verifica $x1_H = x1$ y de ahí que $1_H = 1$.

(3) Sea $x' \in H$ el simétrico de x, entonces se tiene que $xx' = x'x = 1$. Por tanto x' es el simétrico de x en G y así, por la unicidad del elemento simétrico, $x^{-1} = x' \in H$.

■

La siguiente proposición caracteriza de modo sencillo la condición de ser subgrupo.

Proposición 1.2.3 *Sean G un grupo y H un subconjunto no vacío de G. Entonces son equivalentes:*

1. *H es subgrupo de G.*
2. *Para cada par de elementos $x, y \in H$, se tiene $xy^{-1} \in H$.*

DEMOSTRACIÓN.
(1) $\Longrightarrow$ (2) : Sean $x, y \in H$. Entonces, por la Proposición 1.2.2(3), $y^{-1} \in H$. Por tanto $x, y^{-1} \in H$ y por la Proposición 1.2.2(1) se tiene el resultado.
(2) $\Longrightarrow$ (1) : Veremos que H verifica las tres condiciones de la Proposición 1.2.2:

(2) Como H es no vacío, existe al menos un elemento $x \in H$. Por tanto se tiene que $1 = xx^{-1} \in H$.

(3) Como $1 \in H$, entonces para todo $y \in H$ se tiene que $y^{-1} = 1y^{-1} \in H$.

(1) Dados $x, y \in H$, como $y^{-1} \in H$ por el apartado (3), se tiene $xy = x(y^{-1})^{-1} \in H$.

■

Observación 1.2.4 *Dado un grupo G, los conjuntos $\{1\}$ y G son subgrupos de G. Son los llamados subgrupos triviales del grupo G.*

Definición 1.2.5 *Llamaremos subgrupos propios de un grupo G, a aquellos subgrupos distintos de $\{1\}$ y G.*

En el siguiente ejemplo vamos a ver cómo son los subgrupos del grupo aditivo $\mathbb{Z}$.

Ejemplo 1.2.6 *Los subgrupos del grupo $(\mathbb{Z}, +)$ son los conjuntos de la forma*

$$m\mathbb{Z} = \{mx : x \in \mathbb{Z}\},$$

para cada entero m no negativo. Para ello veremos que:

(1) $(m\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}, +)$, y

(2) Todo subgrupo H de $(\mathbb{Z}, +)$, es de la forma $H = m\mathbb{Z}$, para algún entero no negativo m.

Vamos a demostrarlo:

(1) $(m\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Z}, +)$.

(i) Se tiene que $m\mathbb{Z} \neq \emptyset$, ya que $m = m \cdot 1 \in m\mathbb{Z}$, y $m\mathbb{Z} \subseteq \mathbb{Z}$.

(ii) Dados $a, b \in m\mathbb{Z}$, existen $x, y \in \mathbb{Z}$ tales que $a = mx$, $b = my$. Por tanto,

$$a - b = mx - my = m(x - y) \in m\mathbb{Z}.$$

(2) Sea H un subgrupo de $\mathbb{Z}$, entonces pueden ocurrir dos casos:

- *Si $H = \{0\}$, entonces H tiene la forma requerida, ya que en este caso $H = 0\mathbb{Z}$.*
- *Si $H \neq \{0\}$, consideremos m el menor entero positivo en H. Así para todo $n \in H$ se tiene que:*

  (a) Si $n > 0$, por el algoritmo de la división

  $$n = qm + r, \qquad 0 \leq r < m,$$

  donde

  $$qm = \overbrace{m + \cdots + m}^{(q)} \in H, \qquad m \in H.$$

  Por tanto,

  $$r = n - qm \in H.$$

  Así, por la elección que hemos hecho de m, resultará que $r = 0$ y por tanto $n = qm \in m\mathbb{Z}$ de donde $H \subseteq m\mathbb{Z}$.

  (b) Si $n = 0$, entonces $n \in m\mathbb{Z}$, ya que $m\mathbb{Z}$ es subgrupo de $\mathbb{Z}$.

  (c) $n < 0$, entonces tendremos que $-n > 0$ y $-n \in H$, luego por el apartado (a), se tiene que $-n = mx \in m\mathbb{Z}$, para algún entero x. Así $n = m(-x) \in m\mathbb{Z}$.

Así en los apartados (a), (b) y (c) hemos demostrado que $H \subseteq m\mathbb{Z}$. Para la inclusión recíproca sea $y \in m\mathbb{Z}$, es decir existe $x \in \mathbb{Z}$ tal que $y = mx$. Entonces tenemos que:

(i) *Si $x > 0$; $mx = \overbrace{m + \cdots + m}^{(x)} \in H$ ya que $m \in H$.*

(ii) *Si $x = 0$; $mx = 0 \in H$, ya que 0 es el elemento neutro de $(\mathbb{Z}, +)$ y H es subgrupo de $\mathbb{Z}$.*

(iii) *Si $x < 0$; $mx = \overbrace{(-m) + \cdots + (-m)}^{(-x)} \in H$, ya que $-m \in H$ al ser H subgrupo y $m \in H$.*

Luego en todos los casos posibles hemos visto que $m\mathbb{Z} \subseteq H$. Por tanto se tiene $m\mathbb{Z} = H$.

La noción de sistema de generadores de un grupo es también, por su naturaleza de reducción y simplificación, un aspecto importante.

Proposición 1.2.7 *Sea G un grupo y $S \subseteq G$ un subconjunto no vacío. Entonces el conjunto*

$$\langle S \rangle = \left\{ x_1 \cdots x_n : x_i \in S \text{ ó } x_i^{-1} \in S \right\}$$

es un subgrupo de G.

DEMOSTRACIÓN. Se verifica que $\emptyset \neq \langle S \rangle \subseteq G$. Sean $x, y \in \langle S \rangle$, es decir

$$x = x_1 \cdots x_n, \qquad y = y_1 \cdots y_m,$$

donde x_i, $y_j \in S$ ó x_i^{-1}, $y_j^{-1} \in S$, $1 \leq i \leq n$, $1 \leq j \leq m$. Así, tenemos que

$$xy^{-1} = (x_1 \cdots x_n)(y_1 \cdots y_m)^{-1} = (x_1 \cdots x_n)(y_m^{-1} \cdots y_1^{-1}),$$

donde $x_i, y_j \in S$ ó $x_i^{-1}, y_j^{-1} \in S$, $1 \leq i \leq n$, $1 \leq j \leq m$.

■

Definición 1.2.8 *Con la notación anterior, el subgrupo $\langle S \rangle$ será llamado subgrupo generado por el conjunto S.*

Lema 1.2.9 *Sean G un grupo y $\{H_i\}_{i \in I}$ una familia de subgrupos de G. Entonces $\bigcap_{i \in I} H_i$ es un subgrupo de G.*

DEMOSTRACIÓN. Se verifica que:

- $\bigcap_{i \in I} H_i \neq \emptyset$, ya que $1 \in H_i$, $\forall i \in I$ y $\bigcap_{i \in I} H_i \subseteq G$.

- Si $x, y \in \bigcap_{i\in I} H_i$, entonces $x, y \in H_i$, $\forall i \in I$, por tanto, $xy^{-1} \in H_i$, $\forall i \in I$, ya que cada H_i un subgrupo. Así $xy^{-1} \in \bigcap_{i\in I} H_i$.

■

Proposición 1.2.10 *Sean G un grupo y S un subconjunto de G. Entonces*

$$\langle S\rangle = \bigcap_{i\in I} \{H_i : H_i \text{ es un subgrupo de } G,\ S \subseteq H_i\}.$$

DEMOSTRACIÓN. Denotamos

$$H = \bigcap_{i\in I} \{H_i : H_i \text{ es un subgrupo de } G,\ S \subseteq H_i\}.$$

Si $x_1 \cdots x_n \in \langle S\rangle$, entonces $x_i \in S$ o $x_i^{-1} \in S$. Por tanto, al ser cada H_i un subgrupo de G que contiene a S, se tiene que $x_1, \ldots, x_n \in H_i$, $\forall i \in I$ y de ahí que $x_1 \cdots x_n \in H$. Por otra parte, como $\langle S\rangle$ es un subgrupo de G que contiene a S, se tiene que $\langle S\rangle$ es un subgrupo de la familia $\{H_i\}_{i\in I}$ por tanto, $H \subseteq \langle S\rangle$.

■

Observación 1.2.11 *Por la Proposición 1.2.10, $\langle S\rangle$ es el menor subgrupo que contiene a S. Por convenio si $S = \emptyset$ entonces $\langle S\rangle = \{1\}$.*

Como consecuencia de la Proposición 1.2.10 tenemos que:

Corolario 1.2.12 *Si S es un subgrupo de G entonces $\langle S\rangle = S$. En particular $\langle G\rangle = G$.*

Proposición 1.2.13 *Sean G un grupo y S un subconjunto de G. Entonces se verifica:*

$$\langle S\rangle = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : x_i \in S,\ \alpha_i \in \mathbb{Z},\ 1 \leq i \leq n\}.$$

DEMOSTRACIÓN. Denotemos

$$H = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : x_i \in S,\ \alpha_i \in \mathbb{Z},\ 1 \leq i \leq n\}.$$

Entonces tenemos que

(1) $H \subseteq G$.

(2) Si $x, y \in H$, entonces

$$x = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \qquad y = y_1^{\beta_1} \cdots y_m^{\beta_m}.$$

Por tanto, se tiene

$$xy^{-1} = (x_1^{\alpha_1} \cdots x_n^{\alpha_n})\,(y_1^{\beta_1} \cdots y_m^{\beta_m})^{-1} = x_1^{\alpha_1} \cdots x_n^{\alpha_n} y_m^{-\beta_m} \cdots y_1^{-\beta_1} \in H.$$

(3) $S \subseteq H$ ya que para todo $a \in S$, se tiene $a = a^1 \in H$.

(4) H es el subgrupo más pequeño que contiene a S. Para ello, sea B un subgrupo de G que contiene a S. Entonces, para cualquier elemento $a \in H$,

$$a = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in B$$

ya que $x_i \in S$ para todo $1 \leq i \leq n$, $S \subseteq B$ y B es un subgrupo de G. Así, por la Observación 1.2.11 tenemos el resultado.

■

Observación 1.2.14 *Si G es abeliano y usamos la notación aditiva, el subgrupo generado por S es*

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} n_i s_i : s_i \in S,\ n_i \in \mathbb{Z} \right\}.$$

Definición 1.2.15 *Con la notación anterior, el subconjunto S se llama sistema generador de $\langle S \rangle$. Si S es finito, se dice que $\langle S \rangle$ es finitamente generado.*

En el caso que $S = \{a\}$ con $a \in G$, decimos que G es cíclico. Escribiremos $\langle a \rangle$ en lugar de $\langle \{a\} \rangle$. En este caso $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

Definición 1.2.16 *Si G es un grupo con un número finito de elementos, se dice que G es un grupo finito. En caso contrario diremos que G es un grupo infinito.*

Ejemplo 1.2.17 *El subgrupo de S^1 definido por*

$$S^1_{\frac{p}{q}} = \left\{ \exp^{2\pi i \alpha} : \alpha = \frac{p}{q} k,\ k \in \{0, \ldots, q-1\} \right\}$$

es un grupo finito.

Los conceptos de grupo finito y grupo finitamente generado no son equivalentes, como veremos a continuación.

Proposición 1.2.18 *Todo grupo finito es finitamente generado.*

DEMOSTRACIÓN. Sea G un grupo finito, es decir, G como conjunto es finito. Por el Corolario 1.2.12, $\langle G \rangle = G$. Por tanto tendremos que G es finitamente generado.

■

El recíproco de la Proposición 1.2.18 no es cierto como puede verse en el caso del grupo aditivo de los números enteros: $(\mathbb{Z}, +)$ está finitamente generado. En realidad $\mathbb{Z} = \langle 1 \rangle$ ya que para todo $n \in \mathbb{Z}$, se tiene que

- Si $n > 0$, $n = \overbrace{1 + \cdots + 1}^{(n)} \in \langle 1 \rangle$.
- Si $n < 0$, $n = \overbrace{(-1) + \cdots + (-1)}^{(-n)} \in \langle 1 \rangle$.
- Si $n = 0$, siempre tenemos que $0 \in \langle 1 \rangle$, al ser $\langle 1 \rangle$ subgrupo. Sin embargo $\mathbb{Z}$ no es finito.

Veamos algunos ejemplos de grupos finitamente generados.

Ejemplos 1.2.19 *1. El grupo Diédrico D_3: el grupo de los giros y las simetrías de un triángulo equilátero. Este grupo está generado por el giro de ángulo $2\pi/3$ respecto al centro geométrico, y la simetría especular respecto a una altura.*

2. El grupo Diédrico D_4: el grupo de los giros y las simetrías del cuadrado. Este grupo está generado por el giro de ángulo $\pi/2$ respecto al centro geométrico, y la simetría especular respecto a una diagonal. Estos ejemplos se estudiarán con detenimiento al final del Capítulo 4.

3. El grupo de los cuaterniones Q_8. Se conoce con este nombre, y se denota por Q_8, al subgrupo de $GL_2(\mathbb{C})$ generado por las matrices

$$\mathbf{i}=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j}=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k}=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Si denotamos por I_2 la matriz identidad de orden 2, es elemental verificar las siguientes relaciones

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -I_2, \quad \mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}$$

Dados dos subgrupos H y K de un grupo G, podemos considerar el conjunto $HK = \{hk : h \in H,\ k \in K\}$. Este conjunto no es en general un grupo. Sin embargo, bajo ciertas circunstancias sí es subgrupo de G.

Observación 1.2.20 *Siempre se verifica que*

$$H \subseteq HK, \qquad K \subseteq HK.$$

Proposición 1.2.21 *Sean H y K dos subgrupos de un grupo G, entonces*

$$HK \text{ es subgrupo de } G \text{ si y sólo si } HK = KH.$$

DEMOSTRACIÓN.
$\Longrightarrow$: Supongamos que HK es un subgrupo de G y sea $x \in HK$; por tanto x será de la forma $x = hk$ donde $h \in H$, $k \in K$. Así $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in HK$. Pero por definición, existen $h_1 \in H, k_1 \in K$ tales que

$$k^{-1}h^{-1} = h_1k_1.$$

Por tanto,

$$x = \left(x^{-1}\right)^{-1} = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH,$$

luego $HK \subseteq KH$.

Para la otra inclusión, sea $y \in KH$, entonces y será de la forma $y = kh$, con $k \in K$, $h \in H$. Así, al ser H y K subgrupos, se tiene

$$y^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK,$$

y al ser HK un subgrupo, $y = (y^{-1})^{-1} \in HK$. Por tanto hemos demostrado que $KH \subseteq HK$, y de ahí la igualdad.
$\Longleftarrow$: Se trata de demostrar que HK es subgrupo de G.

- $HK \neq \emptyset$, ya que $1 \in HK$.
- Sean $x, y \in HK$. Entonces

  $$x = h_1k_1, \qquad y = h_2k_2,$$

  donde $h_1, h_2 \in H$, $k_1, k_2 \in K$. Así,

  $$xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1}.$$

  Pero, al ser K un subgrupo, tenemos que $k_1k_2^{-1} \in K$. Por tanto existe $k_3 \in K$ tal que $k_1k_2^{-1} = k_3$. Así

  $$xy^{-1} = h_1(k_3h_2^{-1}).$$

  Como $k_3h_2^{-1} \in KH$ y por hipótesis $KH = HK$, podemos escribir $k_3h_2^{-1} = h_3k$, donde $h_3 \in H$, $k \in K$. Así,

  $$xy^{-1} = h_1(h_3k) = (h_1h_3)k \in HK.$$

■

Ejemplo 1.2.22 *Sean $H = m\mathbb{Z}$ y $K = n\mathbb{Z}$ dos subgrupos de $(\mathbb{Z}, +)$ con m y n números enteros no negativos. Como $(\mathbb{Z}, +)$ es un grupo abeliano, se verifica que $H + K = K + H$, luego en virtud de la proposición anterior tenemos que $H + K$ es un subgrupo de $(\mathbb{Z}, +)$. Ahora bien, $H + K \neq \{0\}$, ya que $m = m + 0$ y de ahí que $m \in H + K$. Por tanto $H + K$ es un subgrupo no trivial de $(\mathbb{Z}, +)$, entonces existe $d \in \mathbb{Z}$ tal que $H + K = d\mathbb{Z}$. Veamos que $d = \text{mcd}(m, n)$.*

Como $m = m + 0$ entonces $m \in m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ y así d divide a m. De igual forma se verifica que $n \in m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ y así d divide a n. Por tanto d es divisor de m y de n.

Veamos que es el mayor. Sea $c \in \mathbb{Z}$, tal que c divide a m y a n, es decir $m = cx$, $n = cy$, con $x, y \in \mathbb{Z}$. Por otra parte como $d \in d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$, existirán $a, b \in \mathbb{Z}$, tales que $d = ma + nb$. Por tanto

$$d = ma + nb = cxa + cyb = c(xa + yb),$$

es decir c divide a d, y por tanto podemos afirmar que $d = \text{mcd}(m, n)$.

En particular, de este ejemplo se desprende la llamada Identidad de Bézout: dados $a, b \in \mathbb{Z}$ con $\text{mcd}(a, b) = d$, existen $r, s \in \mathbb{Z}$ tales que $ar + bs = d$.

Proposición 1.2.23 *Dados dos subgrupos H y K de un grupo G, tales que $H \subseteq K$, entonces*

$$HK = K = KH.$$

DEMOSTRACIÓN. Anteriormente hemos demostrado que siempre se verifica $K \subseteq HK$. Veamos la otra inclusión. Cada elemento $x \in HK$ se escribe de la forma $x = hk$ con $h \in H$, $k \in K$. Como $H \subseteq K$, entonces $h \in K$. Por tanto $x = hk \in K$ y así $HK \subseteq K$. Análogamente se verifica $KH = K$.

■

Corolario 1.2.24 *Sean G un grupo, H y K subgrupos de G tales que $H \subseteq K$, entonces HK es subgrupo de G.*

1.3. Orden de un grupo

La finitud en el número de elementos de un grupo es importante para distinguir grupos, no sólo por el aspecto contable, sino también por las propiedades inherentes a un grupo en virtud de su cardinal.

Definición 1.3.1 *Sea G un grupo. Al cardinal de un subgrupo H de G se le llama orden de H y lo denotamos por $o(H)$. En particular, al número de elementos de G se llama orden de G. Un grupo es finito cuando $o(G) < \infty$. En caso contrario decimos que el grupo G es infinito.*

Ejemplo 1.3.2 *Se tiene que*

1. *Tanto* $(\mathbb{Z}, +)$ *como todos sus subgrupos no triviales son grupos infinitos.*
2. *Para cada* $n \geq 1$ *se tiene que* $o(S_n) = n!$.

Definición 1.3.3 *Sea* G *un grupo y* a *un elemento de* G. *Si el subgrupo* $\langle a \rangle$ *es finito, llamamos orden de* a, *y lo denotamos por* $o(a)$, *al orden del subgrupo* $\langle a \rangle$.

Lema 1.3.4 *Sea* G *un grupo y sea* $a \in G$ *tal que* $o(a)$ *es finito. Entonces*

1. *Existe* $k \geq 1$, $k \in \mathbb{Z}$ *tal que* $a^k = 1$.
2. *El orden de* a *es el menor entero natural* $n \geq 1$, *tal que* $a^n = 1$.
3. *Si* $n = o(a)$, *entonces* $\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$.

DEMOSTRACIÓN.

(1) Como $\langle a \rangle$ es finito, la aplicación

$$\begin{array}{ccc} \mathbb{N}\backslash\{0\} & \longrightarrow & \langle a \rangle \\ m & \longmapsto & a^m \end{array}$$

no es inyectiva. Por tanto, existen $r, s \in \mathbb{N}\backslash\{0\}$, con $r < s$ tales que

$$a^r = a^s.$$

Así,

$$1 = a^s(a^r)^{-1} = a^{s-r}.$$

Si llamamos $k = s - r \geq 1$, tenemos

$$a^k = 1 \text{ con } k \geq 1.$$

(2) y (3) Vamos a probar simultáneamente (2) y (3) de la siguiente forma: Por el apartado (1) sabemos que si $o(a)$ es finito, entonces existe $k \geq 1$, tal que $a^k = 1$. Sea n el menor entero natural tal que $a^n = 1$.
Si probamos que $\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$ y que todos los elementos del conjunto de la derecha son distintos tendremos que $o(a) = n$, y quedarán probados (2) y (3).

Siempre se verifica que $\{1, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$. Veamos el recíproco. Sea $x \in \langle a \rangle$, entonces $x = a^k$, $k \in \mathbb{Z}$. Como $\langle a \rangle$ es subgrupo, podemos suponer

que $k > 0$. Por el algoritmo de la división existen $q \in \mathbb{Z}$ y $r \in \mathbb{Z}$ tales que

$$k = nq + r \text{ con } 0 \leq r \leq n-1.$$

Por tanto,

$$x = a^k = a^{nq+r} = (a^n)^q a^r = 1^q a^r = a^r.$$

Así, $x \in \{1, a, \ldots, a^{n-1}\}$ y de ahí que $\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$. Veamos ahora que todos los elementos del conjunto $\{1, a, \ldots, a^{n-1}\}$ son distintos. Para ello, supongamos que existan $r, s \in \mathbb{Z}$, con $0 \leq r < s \leq n-1$ tales que $a^r = a^s$, entonces $a^{s-r} = 1$ con $0 < s - r \leq n - 1 < n$, en contra de la elección de n.

■

Lema 1.3.5 *Sea G un grupo y a un elemento de G de orden finito. Entonces*

1. *Si $n = o(a)$ y $k \in \mathbb{N}$, entonces*

$$a^k = 1 \Longleftrightarrow k \text{ es múltiplo de } n.$$

2. $o(a) = 1 \Longleftrightarrow a = 1$.

3. $o(a^{-1}) = o(a)$ *y por tanto* $o(a^{-1})$ *es finito.*

DEMOSTRACIÓN.

(1) $\Longrightarrow$: Supongamos que k no es múltiplo de n. Entonces, por el algoritmo de la división, existen q, $r \in \mathbb{Z}$ tales que

$$k = nq + r, \qquad 0 < r \leq n - 1.$$

Por tanto, $a^k = a^{nq+r} = (a^n)^q a^r = 1^q a^r = a^r \neq 1$.

$\Longleftarrow$: Supongamos que k es múltiplo de n, es decir, $k = mn$ para algún $m \in \mathbb{Z}$. Entonces $a^k = a^{mn} = (a^n)^m = 1^m = 1$.

(2) $\Longrightarrow$: Si $o(a) = 1$, entonces $a^1 = 1$ y por tanto $a = 1$.
$\Longleftarrow$: Si $a = 1$, entonces $a^1 = 1$, y de ahí que $o(a) = 1$.

(3) Veamos que $\langle a \rangle = \langle a^{-1} \rangle$. Si $x \in \langle a \rangle$, entonces $x = a^k$ para algún $k \in \mathbb{Z}$. Pero $a^k = (a^{-1})^{-k}$, de donde $x \in \langle a^{-1} \rangle$, y de ahí que $\langle a \rangle \subseteq \langle a^{-1} \rangle$. Recíprocamente, si $x \in \langle a^{-1} \rangle$ entonces $x = (a^{-1})^j = a^{-j}$ para algún $j \in \mathbb{Z}$, por tanto $\langle a^{-1} \rangle \subseteq \langle a \rangle$ y de ahí la igualdad.

■

Proposición 1.3.6 *Sea G un grupo y $a \in G$ con $o(a) = n$. Se verifica que*

1. *Si* $x = a^k$, *entonces*
$$o(x) = \frac{n}{\text{mcd}(n,k)}.$$

2. *Si* b *es un elemento de* G *de orden finito y* $ab = ba$, *entonces* $o(ab)$ *es divisor del* $\text{mcm}(o(a), o(b))$. *Si* $\text{mcd}(o(a), o(b)) = 1$ *entonces* $o(ab) = o(a)o(b)$.

DEMOSTRACIÓN.

(1) Sea $d = \text{mcd}(n,k)$, entonces existe $e \in \mathbb{Z}$ tal que $k = ed$. Por tanto
$$x^{\frac{n}{d}} = \left(a^k\right)^{\frac{n}{d}} = a^{\frac{kn}{d}} = a^{en} = (a^n)^e = (1)^e = 1.$$
Entonces por el Lema 1.3.5(1)
$$\frac{n}{d} \text{ es múltiplo de } o(x). \tag{i}$$
Por otra parte, $a^{ko(x)} = \left(a^k\right)^{o(x)} = x^{o(x)} = 1$. Por tanto $ko(x)$ es múltiplo de n. Así $ko(x) = nm$ para cierto $m \in \mathbb{Z}$, es decir, $m\dfrac{n}{o(x)} = k$, por tanto $\dfrac{n}{o(x)}$ divide a k, y como $\dfrac{n}{o(x)}$ divide a n, tendremos que $\dfrac{n}{o(x)}$ divide a $d = \text{mcd}(n,k)$. Así $l\dfrac{n}{o(x)} = d$, para algún $l \in \mathbb{Z}$. En consecuencia $l\dfrac{n}{d} = o(x)$, es decir,
$$o(x) \text{ es múltiplo de } \frac{n}{d}. \tag{ii}$$
De (i) y (ii) podemos afirmar
$$o(x) = \frac{n}{d} = \frac{n}{\text{mcd}(n,k)}.$$

(2) Sean $o(a) = n$, $o(b) = m$ y $M = \text{mcm}(m,n)$. Por tanto, $M = pn = qm$, siendo $p, q \in \mathbb{N}$. Como $ab = ba$, tenemos
$$(ab)^M = a^M b^M = (a^n)^p (b^m)^q = 1^p 1^q = 1.$$
Así, por el Lema 1.3.5(1), tenemos que $o(ab)$ divide a M. En el caso que $\text{mcd}(m,n) = 1$, entonces $M = mn$ y
$$o(ab) \text{ divide a } mn. \tag{iii}$$
Por otra parte, si $o(ab) = s$, entonces $(ab)^s = 1$ y como $ab = ba$, por hipótesis, entonces $a^s b^s = (ab)^s = 1$, luego $a^s = b^{-s}$. En particular, por el Lema 1.3.5(3),
$$o(a^s) = o(b^{-s}) = o((b^s)^{-1}) = o(b^s).$$

Ahora, por el apartado (1), tenemos que

$$\frac{n}{\mathrm{mcd}(n,s)} = o(a^s) = o(b^s) = \frac{m}{\mathrm{mcd}(m,s)}.$$

Es decir, si llamamos

$$h = \frac{n}{\mathrm{mcd}(n,s)} = \frac{m}{\mathrm{mcd}(m,s)},$$

se tiene que h divide a m a n, y al ser éstos primos entre sí, tendremos que $h = 1$, es decir

$$n = \mathrm{mcd}(n,s) \quad \text{y} \quad m = \mathrm{mcd}(m,s).$$

Entonces s es múltiplo de n y m, luego lo es de $M = mn$.
Así

$$o(ab) \text{ es múltiplo de } mn. \tag{iv}$$

Por tanto, de (iii) y (iv) obtenemos que

$$o(ab) = nm = o(a)o(b).$$

■

Como consecuencia inmediata se obtiene el siguiente resultado cuya demostración se propone al lector.

Proposición 1.3.7 *Sea G un grupo y sean H y K subgrupos de G de orden finito. Entonces*

$$\mathrm{card}(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

1.4. Grupos cíclicos

De entre los grupos finitamente generados, los cíclicos son, en muchos aspectos, esenciales para describir grupos finitamente generados más complejos. Eso es especialmente claro en el caso de grupos abelianos, pero también en contextos más generales. Procedemos a establecer sus propiedades elementales.

Definición 1.4.1 *Diremos que un grupo G es cíclico si existe un elemento $a \in G$ tal que $G = \langle a \rangle$.*

Ejemplo 1.4.2 *El grupo $(\mathbb{Z}, +)$ de los números enteros es un grupo cíclico, ya que*

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle.$$

Ejemplo 1.4.3 *$m\mathbb{Z}$ es un grupo cíclico, ya que $m\mathbb{Z} = \langle m \rangle$.*

Lema 1.4.4 *Un grupo finito G es cíclico si y sólo si existe $a \in G$ tal que $o(a) = o(G)$.*

DEMOSTRACIÓN.
$\Longrightarrow$: Si G es cíclico, entonces existe $a \in G$ tal que $G = \langle a \rangle$, por tanto $o(G) = o(a)$.

$\Longleftarrow$: Sea $a \in G$, donde $o(a) = o(G)$, entonces $\langle a \rangle$ es un subgrupo de G que tiene el mismo número de elementos que G, por tanto $G = \langle a \rangle$.

■

Observación 1.4.5 *Si G es infinito, entonces la afirmación del Lema 1.4.4 es falsa. Por ejemplo, $H = \mathbb{Z} \times \{0\}$ es un subgrupo de $G = \mathbb{Z} \times \mathbb{Z}$ con $H \neq \mathbb{Z}$ y sin embargo $o(\mathbb{Z} \times \{0\}) = o(\mathbb{Z} \times \mathbb{Z})$.*

Proposición 1.4.6 *Todo grupo cíclico es abeliano.*

DEMOSTRACIÓN. Sea G un grupo cíclico. Entonces existe $a \in G$ tal que $G = \langle a \rangle$. Veamos que G es abeliano. Si $x, y \in G$, entonces $x = a^k$, $y = a^l$ para ciertos $k, l \in \mathbb{Z}$. Por tanto,

$$xy = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = yx.$$

■

El recíproco de la Proposición 1.4.6 no es cierto, ya que $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ son grupos abelianos pero sin embargo no son cíclicos.

Teorema 1.4.7 *Todo subgrupo de un grupo cíclico es cíclico.*

DEMOSTRACIÓN. Sea G un grupo cíclico, por tanto, existe $a \in G$ tal que $G = \langle a \rangle$. Consideremos H un subgrupo de G. Entonces

- Si $H = \{1\}$ o $H = G$, entonces H es cíclico.
- Sea $H \neq \{1\}$ y $H \neq G$. Entonces existe $x \in H$ con $x \neq 1$, en particular $x \in G = \langle a \rangle$, luego $x = a^r$ para cierto $r \in \mathbb{Z}$. Consideremos m el mínimo entero positivo tal que $a^m \in H$. Vamos demostrar que $H = \langle a^m \rangle$.
  Si $y \in H$, como H es subgrupo de G, $y \in G$. Por tanto existe $n \in \mathbb{Z}$ tal que $y = a^n$. Por el algoritmo de la división en $\mathbb{Z}$, existen $q, r \in \mathbb{Z}$ tales que

$$n = qm + r \text{ con } 0 \leq |r| < m.$$

Entonces $y = a^n = a^{mq+r} = a^{mq}a^r = (a^m)^q a^r$. Es decir, $a^r = (a^m)^{-q}a^n$. Como H un subgrupo y $a^m \in H$ entonces $(a^m)^{-q} \in H$. Por tanto

$$a^r = (a^m)^{-q}a^n \in H,$$

de donde $a^{|r|} \in H$, y por la elección m, $r = 0$. Así

$$y = a^n = a^{mq} = (a^m)^q \in \langle a^m \rangle,$$

luego $H \subseteq \langle a^m \rangle$. Por otro lado, siempre se verifica que $\langle a^m \rangle \subseteq H$. Por tanto $H = \langle a^m \rangle$.

■

1.5. Teorema de Lagrange

En esta sección se establece en el caso de grupos finitos, la relación entre el orden de un subgrupo y el del grupo que lo contiene.

Definición 1.5.1 *Sean G un grupo y $H \subseteq G$ un subgrupo. Definimos en G las siguientes relaciones binarias:*

1. $\forall x, y \in G \quad x\mathcal{R}_H y \iff xy^{-1} \in H.$
2. $\forall x, y \in G \quad x\mathcal{R}^H y \iff x^{-1}y \in H.$

Lema 1.5.2 *Con la notación anterior, las relaciones binarias $\mathcal{R}_H$, $\mathcal{R}^H$, son relaciones de equivalencia sobre G.*

DEMOSTRACIÓN. Lo demostraremos para $\mathcal{R}_H$ y dejaremos el caso de $\mathcal{R}^H$ como ejercicio.

- Reflexiva: Para todo $x \in G$ se tiene que $xx^{-1} = 1 \in H$, por tanto $x\mathcal{R}_H x$.
- Simétrica: Sean $x, y \in G$, tales que $x\mathcal{R}_H y$, entonces $xy^{-1} \in H$. Pero al ser H un subgrupo, se tiene que $(xy^{-1})^{-1} \in H$. Por tanto $yx^{-1} \in H$, y de ahí que $y\mathcal{R}_H x$.
- Transitiva: Sean $x, y, z \in G$ tales que $x\mathcal{R}_H y$ e $y\mathcal{R}_H z$, entonces se tiene $xy^{-1} \in H$ e $yz^{-1} \in H$. Por tanto, al ser H un subgrupo, $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$ y de ahí que $x\mathcal{R}_H z$.

■

Notación 1.5.3 *Dado $a \in G$, denotemos por $[a]_H$ y $[a]^H$ respectivamente las clases de equivalencia que las relaciones $\mathcal{R}_H$ y $\mathcal{R}^H$ determinan en G. Asimismo los conjuntos cocientes serán denotados por $G/\mathcal{R}_H$, $G/\mathcal{R}^H$ respectivamente.*

Lema 1.5.4 *Con la notación anterior, se verifica que*

$$[a]_H = \{ha : h \in H\} \quad y \quad [a]^H = \{ah : h \in H\}.$$

DEMOSTRACIÓN. Notemos

$$Ha = \{ha : h \in H\},$$

donde $a \in G$. Se trata de demostrar que $[a]_H = Ha$. Si $y \in [a]_H$, entonces $y\mathcal{R}_H a$. Por tanto $ya^{-1} \in H$. Así, existe $h \in H$ tal que $ya^{-1} = h$, y de aquí que $y = ha$, con $h \in H$. Por tanto $y \in Ha$. Recíprocamente, sea $y \in Ha$. Entonces existe $h \in H$, tal que $y = ha$, luego $ya^{-1} = h \in H$. Así, $y\mathcal{R}_H a$. Por tanto $y \in [a]_H$. El caso $[a]^H = aH$ es análogo.

■

Definición 1.5.5 *Las clases de equivalencia Ha y aH se llaman respectivamente clases adjuntas por la derecha y por la izquierda de G módulo H.*

Lema 1.5.6 *Sea G un grupo, y sea H un subgrupo de G. Entonces los conjuntos $G/\mathcal{R}_H$ y $G/\mathcal{R}^H$, tienen el mismo cardinal.*

DEMOSTRACIÓN. Para demostrar que los conjuntos $G/\mathcal{R}_H$ y $G/\mathcal{R}^H$ tienen el mismo cardinal, estableceremos una aplicación biyectiva entre ellos. Definimos

$$\begin{aligned} f : G/\mathcal{R}_H &\longrightarrow G/\mathcal{R}^H \\ Ha &\longmapsto a^{-1}H. \end{aligned}$$

Se verifica que:

- f está bien definida y es inyectiva, ya que, dados $a, b \in G$, tenemos

$$Ha = Hb \Longleftrightarrow [a]_H = [b]_H \Longleftrightarrow a\mathcal{R}_H b \Longleftrightarrow ab^{-1} \in H \Longleftrightarrow$$

$$\Longleftrightarrow (a^{-1})^{-1}b^{-1} \in H \Longleftrightarrow a^{-1}\mathcal{R}^H b^{-1} \Longleftrightarrow [a^{-1}]^H = [b^{-1}]^H \Longleftrightarrow$$

$$\Longleftrightarrow a^{-1}H = b^{-1}H \Longleftrightarrow f(Ha) = f(Hb).$$

- f es sobreyectiva, ya que para todo $bH \in G/\mathcal{R}^H$, existe $Hb^{-1} \in G/\mathcal{R}_H$ tal que $f(Hb^{-1}) = bH$.

Por tanto $\text{card}\,(G/\mathcal{R}_H) = \text{card}\,\left(G/\mathcal{R}^H\right)$.

■

Definición 1.5.7 *Sea G un grupo y sea H un subgrupo de G.*

(a) *Si $G/\mathcal{R}_H$ (y por tanto $G/\mathcal{R}^H$) es un conjunto infinito, decimos que H es un subgrupo de G de índice infinito.*

(b) *Si $G/\mathcal{R}_H$ (y por tanto $G/\mathcal{R}^H$) es finito, se llama índice de H en G, y lo denotamos por $[G : H]$, al cardinal (común) de los conjuntos $G/\mathcal{R}_H$ y $G/\mathcal{R}^H$. En este caso decimos que H es un subgrupo de G de índice finito.*

Corolario 1.5.8 *Si G es un grupo de orden finito, entonces todo subgrupo H de G es de índice finito.*

DEMOSTRACIÓN. Consideremos la aplicación,

$$\begin{aligned} G &\longrightarrow G/\mathcal{R}_H \\ a &\longmapsto Ha. \end{aligned}$$

Esta aplicación es sobreyectiva de forma evidente. Por tanto $\text{card}\,(G/\mathcal{R}_H) \leq \text{card}(G)$ y de ahí que $G/\mathcal{R}_H$ sea finito.

■

A continuación vamos a estudiar todo lo anterior en el grupo aditivo de los número enteros. En particular calcularemos el índice de cualquier subgrupo $m\mathbb{Z}$ en $\mathbb{Z}$.

Ejemplo 1.5.9 *Sea $(\mathbb{Z}, +)$ el grupo aditivo de los números enteros y H un subgrupo de $\mathbb{Z}$ distinto de $\{0\}$. Como hemos visto anteriormente, existirá algún entero positivo m tal que $H = m\mathbb{Z}$.*

- *La relación $\mathcal{R}_H$ en este caso vendrá dada por*

$$\forall x, y \in \mathbb{Z}, \qquad x\mathcal{R}_H y \Longleftrightarrow x - y \in H \Longleftrightarrow x - y \in m\mathbb{Z}.$$

- *Las clases que la relación $\mathcal{R}_H$ determina en $\mathbb{Z}$ serán*

$$[x]_H = H + x = m\mathbb{Z} + x, \qquad x \in \mathbb{Z}.$$

- *Vamos a calcular el conjunto cociente $\mathbb{Z}/\mathcal{R}_H$. Se tiene que*

$$\mathbb{Z}/\mathcal{R}_H = \{H + 0, H + 1, \ldots, H + (m-1)\}.$$

Sea $x \in \mathbb{Z}$. Por el algoritmo de la división obtenemos

$$x = qm + r, \qquad 0 \leq r \leq m - 1.$$

Así $x - r = qm \in H$, luego $x\mathcal{R}_H r$, esto es, $H + x = H + r$. Luego

$$[x]_H = [r]_H, \text{ donde } 0 \leq r \leq m - 1.$$

Además, los elementos del segundo miembro son distintos, pues si

$$H + k = H + l, \qquad 0 \leq k < l \leq m - 1,$$

tendríamos que $l\mathcal{R}_H k$, es decir, $l - k \in H = m\mathbb{Z}$ con $1 \leq l - k < m$, lo cual es imposible. Así $[\mathbb{Z} : m\mathbb{Z}] = m$.

Por tanto podemos concluir que $\mathbb{Z}$ es un grupo infinito, finitamente generado, cuyos subgrupos no nulos tienen índice finito.

Lema 1.5.10 *Sea H un subgrupo de G, y sea $x \in G$. Entonces las aplicaciones*

$$f: \begin{array}{ccc} H & \longrightarrow & Hx \\ h & \longmapsto & hx \end{array} \qquad y \qquad g: \begin{array}{ccc} H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array}$$

son biyectivas.

DEMOSTRACIÓN. Haremos la demostración para la aplicación f. De igual forma se demuestra que g es biyectiva.

- f es inyectiva, ya que si $f(h_1) = f(h_2)$ entonces $h_1x = h_2x$. Por tanto, $h_1 = h_2$.
- f es sobreyectiva, ya que para todo $hx \in Hx$, existe $h \in H$ tal que $f(h) = hx$.

■

Observaciones 1.5.11 *De la proposición anterior, tenemos que:*

(a) Dado $x \in G$ existe una biyección entre Hx y xH. Sin embargo éstos pueden ser diferentes.

(b) Si $o(H)$ es finito, se verifica que

$$\text{card}(Hx) = \text{card}(xH) = \text{card}(H) = o(H).$$

Teorema 1.5.12 (Teorema de Lagrange) *Sea G un grupo finito, y sea H un subgrupo de G. Entonces se verifica que:*

$$o(G) = o(H)[G : H].$$

DEMOSTRACIÓN. Consideramos la relación $\mathcal{R}_H$ definida en G. Al ser $\mathcal{R}_H$ una relación de equivalencia, G es unión disjunta de las clases de equivalencia Hx, y al ser G un grupo finito, habrá sólo un número finito. Sean éstas

$$Hx_1, \ldots, Hx_r,$$

donde se verificará que el número de elementos de G es la suma de los cardinales de estas clases, es decir

$$\text{card}(G) = \sum_{i=1}^{r} \text{card}(Hx_i), \qquad Hx_i \in G/\mathcal{R}_H.$$

Por el Lema 1.5.10, se verifica que

$$\text{card}(Hx_i) = \text{card}(H) = o(H),$$

entonces

$$\text{card}(G) = \text{card}(H) \cdot \text{card}\left(G/\mathcal{R}_H\right).$$

Por tanto

$$o(G) = o(H)[G : H],$$

ya que el número de clases que la relación $\mathcal{R}_H$ determina en G es, por definición, el índice de H en G.

■

Vamos a ver a continuación algunas consecuencias y aplicaciones del Teorema de Lagrange.

Corolario 1.5.13 *El orden de todo subgrupo de un grupo finito es divisor del orden del grupo.*

En general el recíproco del Corolario anterior no es cierto, como veremos en el caso del grupo A_4. El orden de A_4 es 12 y sin embargo no tiene subgrupos de orden 6.

Corolario 1.5.14 *El orden de todo elemento de un grupo finito es divisor del orden del grupo.*

DEMOSTRACIÓN. Sea G un grupo finito y sea $a \in G$. Como se verifica que $\langle a \rangle \subseteq G$, es un subgrupo de G y $o(a) = o(\langle a \rangle)$, entonces, por el Corolario 1.5.13, se tiene que $o(a)$ divide al $o(G)$.

■

Ejemplo 1.5.15 *En* $(\mathbb{Z}_6, +)$ *tenemos que* $o([0]) = 1$, $o([1]) = 6$, $o([2]) = o([4]) = 3$ *y* $o([3]) = o([5]) = 2$.

Corolario 1.5.16 *Todo grupo finito de orden primo es cíclico y sus únicos subgrupos son los triviales.*

DEMOSTRACIÓN. Sea G un grupo finito de orden p, siendo p un número primo. Sea $a \in G$, donde $a \neq 1$. Consideremos el subgrupo $\langle a \rangle$. Entonces el Corolario 1.5.14 afirma que $o(a)$ divide a p, siendo p primo. Por tanto tenemos dos posibilidades:

- $o(a) = 1$, que es contradictorio con el hecho de que $a \neq 1$.
- $o(a) = p$ y por consiguiente $G = \langle a \rangle$, es decir G es cíclico.

Finalmente, sea H cualquier subgrupo del grupo G. Entonces por el Teorema de Lagrange, tenemos que $o(H)$ es divisor de $o(G) = p$. Así tendremos que:

- Si $o(H) = 1$, entonces $H = \{1\}$.
- Si $o(H) = p$, entonces $H = G$.

Por tanto los únicos subgrupos de G son los triviales.

■

Como hemos dicho anteriormente, el recíproco del Teorema de Lagrange no se verifica siempre, es decir, para todo divisor m del orden del grupo, existe un subgrupo de orden m. Sin embargo esto sí es cierto en los grupos cíclicos, como vamos a ver a continuación.

Proposición 1.5.17 *Sea G un grupo cíclico con $n = o(G)$. Entonces para cada divisor m de n, existe un único subgrupo de G de orden m. Además este subgrupo es cíclico.*

DEMOSTRACIÓN. Sea $a \in G$ tal que $G = \langle a \rangle$. Si m es divisor de n, existe $d \in \mathbb{N}$ tal que $n = md$. Consideremos el subgrupo $H = \langle a^d \rangle$. Por la Proposición 1.3.6, tenemos que

$$o(a) = \frac{n}{\text{mcd}(n,d)} = \frac{n}{d} = m.$$

Por tanto, $o(H) = m$. Vamos a demostrar que cualquier subgrupo de orden m es de esta forma.

Sea L un subgrupo de G tal que $o(L) = m$. Consideremos l el menor entero positivo tal que $a^l \in L$ (existe ya que $L \subseteq G = \langle a \rangle$). Utilizando el mismo razonamiento que en la demostración del Teorema 1.4.7, tenemos que $L = \langle a^l \rangle$. Por tanto

$$1 = \left(a^l\right)^m = a^{lm}$$

y así, por el Lema 1.3.5(1), afirmamos que n divide a lm. Por tanto existe $e \in \mathbb{Z}$ tal que $ne = lm$. Entonces

$$a^l = \left(a^{\frac{n}{m}}\right)^e = \left(a^d\right)^e,$$

de donde $\langle a^l \rangle \subseteq \langle a^d \rangle$. Así tenemos que L es un subgrupo de H tal que $o(L) = o(H)$. Por tanto $H = L$.

■

1.6. Subgrupos normales. Grupo cociente

Al trabajar con cualquier clase de objetos en Álgebra, es importante hallar relaciones de equivalencia tales que los conjuntos cocientes admitan, de modo natural, una estructura del tipo de la de los objetos iniciales. En el caso de los grupos, si H es un subgrupo de un grupo G, los conjuntos cocientes $G/\mathcal{R}_H$ y $G/\mathcal{R}^H$ no admiten, en general, estructura de grupo de modo natural. Estudiaremos aquí los subgrupos H para los cuales esto es posible.

Definición 1.6.1 *Sea S un subconjunto no vacío de un grupo G y a un elemento de G. Llamamos conjugado de S por a al conjunto*

$$a^{-1}Sa = \left\{a^{-1}xa : x \in S\right\}.$$

Lema 1.6.2 *Sea G un grupo y S un subconjunto de G, entonces se verifica:*

1. $y \in a^{-1}Sa \iff aya^{-1} \in S$.
2. *Si S es un subgrupo de G, entonces $a^{-1}Sa$ es un subgrupo de G.*
3. *Si $S \subseteq T$, entonces $a^{-1}Sa \subseteq a^{-1}Ta$.*

DEMOSTRACIÓN.

(1) $y \in a^{-1}Sa \iff y = a^{-1}xa, \quad x \in S \quad \iff aya^{-1} = x \in S.$

(2) $a^{-1}Sa \neq \emptyset$, ya que al ser S subgrupo, $1 \in S$ y de ahí que

$$1 = a^{-1}1a \in a^{-1}Sa.$$

Si $y_1, y_2 \in a^{-1}Sa$, entonces existen $x_1, x_2 \in S$ tales que

$$y_1 = a^{-1}x_1a, \qquad y_2 = a^{-1}x_2a.$$

Así

$$y_1y_2^{-1} = (a^{-1}x_1a)(a^{-1}x_2a)^{-1} = (a^{-1}x_1a)(a^{-1}x_2^{-1}a) =$$
$$= (a^{-1}x_1x_2^{-1}a) = a^{-1}(x_1x_2^{-1})a \in a^{-1}Sa,$$

ya que $x_1x_2^{-1} \in S$, al ser S un subgrupo.

(3) Si $y \in a^{-1}Sa$, entonces existe $x \in S$ tal que $y = a^{-1}xa$. Pero al ser S subconjunto de T, se tiene que $x \in T$ y de ahí que $a^{-1}xa \in a^{-1}Ta$.

■

Proposición 1.6.3 *Sean G un grupo y sea H un subgrupo de G. Entonces las siguientes condiciones son equivalentes:*

1. $Ha = aH$ *para cada* $a \in G$.

2. $H = a^{-1}Ha$ *para cada* $a \in G$.

3. *Para cada par de elementos* $a, b \in G$ *tales que* $ab \in H$ *entonces* $ba \in H$.

DEMOSTRACIÓN.
(1) $\Longrightarrow$ (2): Si $y \in a^{-1}Ha$, entonces $y = a^{-1}ha$, con $h \in H$. Así tenemos que $ay = ha$, de donde $ay \in Ha$. Pero por hipótesis $Ha = aH$, entonces existe $h' \in H$ tal que $ay = ah'$, de donde $y = h'$. Así $y \in H$. Con esto hemos demostrado que

$$a^{-1}Ha \subseteq H.$$

Recíprocamente sea $h \in H$, entonces $ah \in aH$. Por hipótesis tenemos que $aH = Ha$, luego existe $h' \in H$ tal que $ah = h'a$, o lo que es lo mismo, $h = a^{-1}h'a$. Por tanto $H \subseteq a^{-1}Ha$.

(2) $\Longrightarrow$ (3): Sean $a, b \in G$, tales que $ab \in H$. Entonces

$$ba = (a^{-1}a)(ba) = a^{-1}(ab)a \in a^{-1}Ha = H.$$

(3) $\Longrightarrow$ (1) : Sea $x \in Ha$. Entonces $x = ha$ para algún $h \in H$. Por tanto $xa^{-1} = h \in H$. Así, aplicando la hipótesis, $a^{-1}x \in H$, es decir, existe $h' \in H$ tal que $a^{-1}x = h'$, de donde $x = ah' \in aH$. Por consiguiente $Ha \subseteq aH$. La otra inclusión se demuestra de forma análoga.

■

Definición 1.6.4 *Diremos que un subgrupo* H *de un grupo* G *es subgrupo normal, y se denotará por* $H \lhd G$, *si verifica una cualquiera y por tanto todas las condiciones de la Proposición 1.6.3.*

Observaciones 1.6.5 *Se tiene que:*

1. *Evidentemente la condición (1) de la Proposición 1.6.3 equivale a decir que* $\mathcal{R}_H = \mathcal{R}^H$. *En particular, si* H *es un subgrupo normal de* G, *tendremos que* $G/\mathcal{R}_H = G/\mathcal{R}^H$ *y denotaremos ambos cocientes por* G/H.

2. *Para probar que* H *es un subgrupo normal de* G *basta ver que*

$$a^{-1}Ha \subseteq H \quad \text{para todo } a \in G.$$

Vamos a verlo: si $a^{-1}Ha \subseteq H$ *para cada* $a \in G$, *entonces como* $a^{-1} \in G$, *tendremos que* $aHa^{-1} \subseteq H$. *Luego para todo* $y \in H$ *se tiene que* $aya^{-1} \in H$. *Por otro lado, se tiene que* $y = a^{-1}(aya^{-1})a$. *Por tanto* $y \in a^{-1}Ha$ *y así* $H \subseteq a^{-1}Ha$, *obteniéndose la igualdad.*

En cualquier grupo G, los subgrupos $\{1\}$ y G son normales en G, ya que $a\{1\} = a = \{1\}a$ para todo $a \in G$. (y de ahí podemos obtener que $G/\{1\} = G$). También podemos afirmar que G es un subgrupo normal de G, ya que $a^{-1}Ga \subseteq G$ para todo $a \in G$.

Vamos a enunciar dos resultados sobre propiedades que verifican los subgrupos normales y que nos serán de utilidad más adelante. La demostración se deja como ejercicio para el lector.

Lema 1.6.6 *Sea G un grupo, y sean H y K subgrupos de G tal que H es subgrupo normal de G. Entonces HK es subgrupo de G.*

Lema 1.6.7 *Sea N un subgrupo normal de un grupo G y sean H y K subgrupos de G tales que H es subgrupo normal de K. Entonces NH es subgrupo normal de NK.*

Definición 1.6.8 *Diremos que dos subgrupos H, K de G son conjugados si existe $g \in G$ tal que $g^{-1}Hg = K$.*

Observación 1.6.9 *Como la aplicación conjugar por g es una biyección en G, se tiene que $o(H) = o(g^{-1}Hg)$.*

Definición 1.6.10 *Decimos que un grupo G es simple, si $\{1\}$ y G son sus únicos subgrupos normales.*

Los ejemplos más sencillos de grupos simples son los de orden primo, ya que hemos visto en el Corolario 1.5.16 que los únicos subgrupos de un grupo de orden primo son los triviales. Veamos otros ejemplos de subgrupos normales.

Ejemplos 1.6.11

1. *Todo subgrupo de un grupo abeliano es normal, ya que en un grupo G es abeliano, se verifica que $ab = ba$ para todo a, $b \in G$. Por tanto se cumple la afirmación* (3) *de la Proposición 1.6.3.*

2. *Como todo grupo cíclico es abeliano, en particular se tendrá que todo subgrupo de un grupo cíclico es normal.*

3. *Si G es un grupo y H es un subgrupo de G con índice 2, entonces H es un subgrupo normal de G. En efecto, como las clases por la derecha módulo H constituyen una partición de G, sólo hay dos, y una de ellas es H, la otra ha de ser el complementario $\{g \in G : g \notin H\}$. El mismo argumento vale para las clases por la izquierda y en consecuencia se tiene que los conjuntos cocientes $G/\mathcal{R}_H$ y $G/\mathcal{R}^H$ son iguales y por la condición* (1) *de la Proposición 1.6.3 tendremos el resultado.*

4. *El subgrupo $SL_n(\mathbb{R})$ es un un subgrupo normal de $GL_n(\mathbb{R})$. Para verlo utilizamos el hecho de que*

$$\det(ab) = \det(a)\det(b) = \det(b)\det(a) = \det(ba).$$

Proposición 1.6.12 *Sean G un grupo, H un subgrupo normal de G. En el conjunto G/H definimos la siguiente operación interna*

$$\begin{array}{rcl} G/H \times G/H & \longrightarrow & G/H \\ (aH, bH) & \longmapsto & (ab)H. \end{array}$$

Entonces $(G/H, \cdot)$ es un grupo. Además si H es un subgrupo de G de índice finito, entonces

$$o(G/H) = [G : H] = \frac{o(G)}{o(H)}.$$

DEMOSTRACIÓN. La operación definida verifica:

- Es operación interna: dados aH, $bH \in G/H$, como $a, b \in G$, se tiene que $ab \in G$, de donde $(aH)(bH) = (ab)H \in G/H$.

- Está bien definida: Sean $a_1H = a_2H$, $b_1H = b_2H$; deberemos demostrar que

$$(a_1b_1)H = (a_2b_2)H,$$

o lo que es lo mismo

$$(a_1b_1)^{-1}(a_2b_2) \in H, \text{ esto es, } b_1^{-1}a_1^{-1}a_2b_2 \in H.$$

Pero si $a_1H = a_2H$ entonces $a_1\mathcal{R}^H a_2$ y por tanto $a_1^{-1}a_2 \in H$. De igual forma si $b_1H = b_2H$, se tiene que $b_1\mathcal{R}^H b_2$ y por tanto $b_1^{-1}b_2 \in H$. Denotemos $h = a_1^{-1}a_2$ y $h' = b_1^{-1}b_2$. Por ello

$$b_1^{-1}(a_1^{-1}a_2)b_2 = b_1^{-1}hb_2 = b_1^{-1}b_2(b_2^{-1}hb_2) = h'(b_2^{-1}hb_2).$$

Pero $h' \in H$ y al ser H un subgrupo normal de G, se tiene que $b_2^{-1}hb_2 \in b_2^{-1}Hb_2 = H$, luego $b_1^{-1}a_1^{-1}a_2b_2 \in H$, como queríamos probar.

- Asociativa:

$$(aH)[(bH)(cH)] = (aH)[(bc)H] = [a(bc)]H =$$

$$= [(ab)c]H = [(ab)H](cH) = [(aH)(bH)](cH).$$

- Existencia de elemento neutro: como

$$(aH)H = (aH)(1H) = (a1)H = (aH)$$

y

$$H(aH) = (1H)(aH) = (1a)H = (aH),$$

entonces el elemento neutro en G/H, respecto de la operación definida, es H.

- Existencia de elemento inverso: dado $aH \in G/H$, se verifica que:

$$(aH)(a^{-1}H) = (aa^{-1})H = 1H = H$$

y

$$(a^{-1}H)(aH) = (a^{-1}a)H = 1H = H,$$

lo que prueba que $(a^{-1}H)$ es el inverso de (aH), es decir $(aH)^{-1} = a^{-1}H$.

Por último, si H es un subgrupo de índice finito en G, se verifica, utilizando el Teorema de Lagrange,

$$o(G/H) = \text{card}\,(G/H) = [G : H] = \frac{o(G)}{o(H)}.$$

■

Definición 1.6.13 *Si G es un grupo y H es un subgrupo normal de G, entonces al grupo $(G/H, \cdot)$ se le denomina grupo cociente de G por el subgrupo H.*

Ejemplos 1.6.14 *Como ejemplos de grupos cocientes podemos presentar a los siguientes, cuya demostración se presentará en el Capítulo 2.*

1. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R} \setminus \{0\}$. *(Ver 2.4.5).*
2. $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. *(Ver 2.4.6).*
3. $\mathbb{Q}/\mathbb{Z}$. *Este ejemplo es notable, porque es infinito, pero todo elemento tiene orden finito. Para ver ambas afirmaciones, observemos que $a, b \in \mathbb{Q}$ representan a la misma clase en $\mathbb{Q}/\mathbb{Z}$ si y sólo si $a - b \in \mathbb{Z}$. En vista de esto, es claro que, para todo $n \in \mathbb{N}$, $\left[\frac{1}{n}\right]$ es un elemento de orden n, por lo que $\left\{\left[\frac{1}{n}\right]\right\}_{n\geq 2}$ es un subconjunto infinito de $\mathbb{Q}/\mathbb{Z}$. Asimismo, dado $a \in \mathbb{Q}/\mathbb{Z}$, $a = \left[\frac{p}{q}\right]$ con $p, q \in \mathbb{Z}$ coprimos, de donde $o(a) = |q|$.*

4. $\mathbb{R}/\mathbb{Z} \cong S^1$. *El ejemplo anterior es un subgrupo propio de éste, ya que existen infinitos elementos en* $\mathbb{R} \setminus \mathbb{Q}$, *y las clases de estos tienen orden infinito en* $\mathbb{R}/\mathbb{Z}$. *Bajo la identificación con* S^1, $\mathbb{Q}/\mathbb{Z}$ *corresponde a los complejos de norma 1 con argumento un múltiplo racional de* 2π.

5. $\mathbb{R}/\mathbb{Q}$. *Observemos que en este caso toda clase está representada por un irracional, de lo que se desprende que todo elemento tiene orden infinito. No existe una manera intuitiva de representar este grupo. Es más, aceptando el axioma de la elección, se puede probar que es un conjunto no medible.*

A continuación vamos a estudiar los subgrupos de un grupo cociente y qué propiedades conserva del grupo G.

Proposición 1.6.15 *Sean G un grupo, H un subgrupo normal de G, entonces se verifica:*

1. *Si K es un subgrupo de G, $H \subseteq K$, entonces K/H es subgrupo de G/H.*

2. *Si M es un subgrupo de G/H, entonces existe un subgrupo K de G tal que $H \subseteq K$ y $M = K/H$.*

DEMOSTRACIÓN.

(1)
- H es un subgrupo normal de K ya que H un subgrupo normal de G. Así tiene sentido considerar el grupo K/H.
- $K/H \subseteq G/H$, de forma inmediata.
- $K/H \neq \emptyset$, ya que $1 \in K$, y por tanto $1H \in K/H$.
- Sean $(xH), (yH) \in K/H$, donde $x, y \in K$. Entonces

$$(xH)(yH)^{-1} = (xH)(y^{-1}H) = (xy^{-1})H \in K/H,$$

ya que $xy^{-1} \in K$, al ser K un subgrupo de G.

(2) Sea M un subgrupo de G/H, y consideremos $K = \{x \in G : xH \in M\}$. Veamos que K verifica las propiedades enunciadas.

- $H \subseteq K$, $K \neq \emptyset$, ya que para todo $h \in H$ se tiene que $hH = H$. Por otra parte $1H \subseteq M$, al ser M un subgrupo de G/H y $1H$ el elemento neutro de G/H. Luego $hH \in M$ y por tanto $h \in K$. Así $H \subseteq K$ y $K \neq \emptyset$.
- K es subgrupo de G, ya que dados $x, y \in K$, tendremos que xH, $yH \in M$, y como M es un subgrupo de G/H, tendremos que $(xH)(yH)^{-1} \in M$. Así,

$$(xy^{-1})H = (xH)(y^{-1}H) = (xH)(yH)^{-1} \in M,$$

y por tanto $xy^{-1} \in K$, luego K es un subgrupo de G.

- $M = K/H$, ya que si $(xH) \in K/H$, con $x \in K$, entonces $xH \in M$. Por tanto $K/H \subseteq M$. En el otro sentido, sea $xH \in M$, entonces $x \in K$, luego $xH \in K/H$ y así $M \subseteq K/H$. Por tanto, podemos afirmar que $M = K/H$.

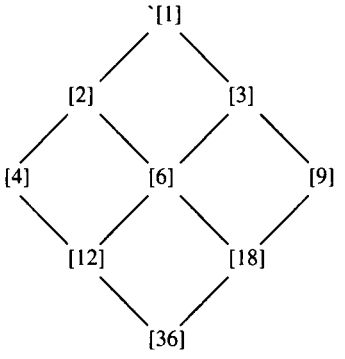
■

Observación 1.6.16 *Así queda demostrado que existe una biyección entre los subgrupos de G que contienen a H y los subgrupos de G/H.*

Vamos a ver un par de ejemplos de correspondencia de subgrupos en cocientes de grupos.

Ejemplo 1.6.17 *Vamos a presentar los subgrupos del grupo $\mathbb{Z}/343\mathbb{Z}$. Por la Proposición 1.6.15, los subgrupos de $\mathbb{Z}/343\mathbb{Z}$ se corresponden con los subgrupos de $\mathbb{Z}$ que contienen al subgrupo $343\mathbb{Z}$. Como todo subgrupo de $\mathbb{Z}$ es de la forma $n\mathbb{Z}$, éstos son los subgrupos de $\mathbb{Z}$ generados por divisores de 343, es decir, $\mathbb{Z}, 7\mathbb{Z}, 49\mathbb{Z}, 343\mathbb{Z}$. Por lo tanto, los subgrupos de $\mathbb{Z}/343\mathbb{Z}$, y sus relaciones de inclusión, quedan descritos mediante el siguiente diagrama, donde las líneas verticales indican inclusión (de abajo arriba):*

Ejemplo 1.6.18 *Este ejemplo es análogo al anterior, pero para el grupo $\mathbb{Z}/36\mathbb{Z}$. Observemos que, en este caso, el grupo tiene subgrupos no comparables por la relación de inclusión, como se aprecia en el diagrama:*



Veamos ahora cómo se comporta la condición de normalidad respecto a cocientes de grupos.

Proposición 1.6.19 *Sea G un grupo, sea H un subgrupo normal de G, y sea K un subgrupo de G que contiene a H. Entonces se verifica que K es subgrupo normal de G si y sólo si K/H es subgrupo normal de G/H.*

DEMOSTRACIÓN. Sean $xH, yH \in G/H$ tales que $(xH)(yH) \in K/H$. Entonces $(xy)H \in K/H$, donde $xy \in K$. Pero por hipótesis, K es un subgrupo normal. Entonces por la Proposición 1.6.3(3) tendremos $yx \in K$. Por tanto $(yH)(xH) \in K/H$ y así, de nuevo por la Proposición 1.6.3(3), K/H es un subgrupo normal de G/H.

Recíprocamente sea K un subgrupo de G, y $a, b \in G$ tales que $ab \in K$. Entonces $(aH)(bH) = (ab)H \in K/H$. Como por hipótesis, K/H es un subgrupo normal y $(aH)(bH) \in K/H$, por la Proposición 1.6.3(3) tenemos que $(bH)(aH) \in K/H$. Por tanto $(ba)H = (bH)(aH) \in K/H$. Así $ba \in K$ y de ahí podemos afirmar, por la Proposición 1.6.3(3), que K es un subgrupo normal de G.

■

Proposición 1.6.20 *Sea G un grupo, y sea H un subgrupo normal de G. Entonces G/H es cíclico si G es cíclico.*

DEMOSTRACIÓN. Si G es un grupo cíclico, entonces existe $a \in G$ tal que $G = \langle a \rangle$. Se trata de demostrar que $G/H = \langle aH \rangle$.
Sea $y \in G/H$, es decir $y = xH$, con $x \in G$. Entonces $x = a^k$ para algún $k \in \mathbb{Z}$. Así $y = a^k H = (aH)^k$, de donde $y \in \langle aH \rangle$. Por tanto $G/H \subseteq \langle aH \rangle$. Por otra parte, como siempre se verifica que $\langle aH \rangle \subseteq G/H$, entonces podemos afirmar que que $G/H = \langle aH \rangle$.

■

El recíproco de la Proposición 1.6.20 es falso: $0 \times \mathbb{Z}$ es un subgrupo normal de $\mathbb{Z} \times \mathbb{Z}$, y $(\mathbb{Z} \times \mathbb{Z})/(0 \times \mathbb{Z})$ es un grupo cíclico infinito, pero $\mathbb{Z} \times \mathbb{Z}$ no es cíclico.

Por último vamos a ver en el paso al cociente también se conserva la condición de ser abeliano.

Proposición 1.6.21 *Sea G un grupo abeliano y H un subgrupo normal de G, entonces G/H es también abeliano.*

DEMOSTRACIÓN. Sean xH, $yH \in G/H$, entonces

$$(xH)(yH) = (xy)H = (yx)H = (yH)(xH)$$

ya que $xy = yx$ al ser G un grupo abeliano.

■

El recíproco de la Proposición 1.6.21 es falso: $\langle (1,2,3) \rangle$ es un subgrupo normal de S_3, ya que tiene orden 3, y por tanto su índice es 2. Asimismo, $S_3/\langle (1,2,3) \rangle$ tiene orden dos, y por tanto es abeliano. Pero S_3 no es abeliano.

En el siguiente ejemplo particularizamos los conceptos expuestos al grupo aditivo $(\mathbb{Z}, +)$.

Ejemplo 1.6.22 *Cualquier subgrupo H de $(\mathbb{Z}, +)$ es de la forma $H = m\mathbb{Z}$, para un cierto entero positivo m. Como $(\mathbb{Z}, +)$ es un grupo abeliano, resultará que todo subgrupo es normal. Así tendrá sentido considerar el grupo $\mathbb{Z}/m\mathbb{Z}$. La operación en el conjunto cociente viene dada por*

$$\begin{array}{rcl} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ (a + m\mathbb{Z}, b + m\mathbb{Z}) & \longmapsto & (a+b) + m\mathbb{Z}. \end{array}$$

Al ser $(\mathbb{Z}, +)$ un grupo cíclico, tendremos que $\mathbb{Z}/m\mathbb{Z}$ también es cíclico. De hecho, se tiene $\mathbb{Z}/m\mathbb{Z} = \langle 1 + m\mathbb{Z} \rangle$. Así, como $(\mathbb{Z}, +)$ es un grupo abeliano, entonces $\mathbb{Z}/m\mathbb{Z}$ es también abeliano.

Recordemos que al ser

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\},$$

entonces podemos afirmar que $o(\mathbb{Z}/m\mathbb{Z}) = m$.

Así podemos afirmar que $(\mathbb{Z}/m\mathbb{Z}, +)$ es un grupo cíclico de orden m.

Como veremos en el próximo capítulo, los grupos cíclico finitos son exactamente los grupos de la forma $\mathbb{Z}/m\mathbb{Z}$, con $m \in \mathbb{Z}^+$.

1.7. Ejercicios

1. Determinad si cada una de las definiciones de la operación $*$ dada a continuación, da una ley de composición interna en el conjunto dado.

   a) En $\mathbb{Z}^+$ definimos $a * b = a^b$.

   b) En $\mathbb{Z}^+$ definimos $a * b = c$, donde c es el menor entero mayor que a y b.

   c) En $\mathbb{Z}^+$ definimos $a * b = c$, donde c es al menos 5 unidades mayor que $a + b$.

   d) La división en $\mathbb{Q} \setminus \{0\}$.

   e) La división en Q.

2. Sobre el intervalo $G = (-1, 1)$ de la recta real se define la siguiente operación
$$x * y = \frac{x + y}{1 + xy}.$$
Demostrad que $(G, *)$ es un grupo abeliano.

3. Sea $G = \{(a, b) : a \in \mathbb{Q} \setminus \{0\},\ b \in \mathbb{Q}\}$. Se define en G la siguiente ley interna
$$(a, b) * (c, d) = (ac, ad + b).$$

   a) Probad que (G,*) es un grupo no abeliano.

   b) Hallad $(x, y) \in G$ tal que $(1, 2) * (x, y) * (2, 3)^{-1} = (5, 6)$.

4. En $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ consideramos la operación $\circ$ definida así:
$$x \circ y = \begin{cases} xy & \text{si} \quad x > 0 \\ \frac{x}{y} & \text{si} \quad x < 0 \end{cases}.$$
Probad que $(\mathbb{R}^*, \circ)$ es un grupo.

5. Sean $\mathbb{Q}[i]$ y $\mathbb{Z}[i]$ los subconjuntos de los números complejos definidos por
$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \qquad \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}.$$
Probad que:

   a) $\mathbb{Z}[i]$, $\mathbb{Q}[i]$ son grupos respecto de la suma de números complejos.

   b) $(\mathbb{Q}[i] \setminus \{0\}, \cdot)$ es un grupo, pero $(\mathbb{Z}[i] \setminus \{0\}, \cdot)$ no lo es.

6. Sea $n \in \mathbb{Z}$ y consideremos el conjunto
$$G_n = \left\{ \cos(\frac{2\pi k}{n}) + i\text{sen}\,(\frac{2\pi k}{n}) : k \in \mathbb{Z} \right\} \subseteq \mathbb{C}.$$

a) Probad que $(G_n, \cdot)$ es un grupo.

b) Probad que G_n tiene un número finito de elementos.

7. Estudiad las isometrías del plano que dejan invariante un rectángulo. Si se define en este conjunto la operación composición de movimientos, comprobad que tiene estructura de grupo. Este grupo se llama Grupo de Klein.

8. Sea G un grupo. Demostrad que se verifica:

a) Si $x^2 = 1$ para cada $x \in G$, entonces G es un grupo abeliano.

b) Si $(ab)^2 = a^2b^2$ para cada $a, b \in G$, entonces G es un grupo abeliano.

9. Dad un ejemplo que muestre que la unión de dos subgrupos H y K de G no es en general un subgrupo de G.

10. Dad ejemplos de:

a) Un grupo infinito cuyos cocientes no triviales sean todos finitos.

b) Un grupo infinito cuyos elementos sean todos de orden finito.

11. Sea G un grupo finito en el que se cumple que la unión de dos subgrupos cualesquiera es también un subgrupo de G. Demostrad que G es cíclico y que su orden es potencia de un número primo.

12. Sea G un grupo finito en el que se cumple que para cualesquiera dos subgrupos H, K se tiene H es subgrupo de K o K es subgrupo de H. Demostrad que G es cíclico y que su orden es potencia de un número primo.

13. Sea G un grupo y H el siguiente subgrupo de G

$$H = \left\{x^2 : x \in G\right\}.$$

Demostrad que H es normal y G/H es abeliano.

14. Demostrad que todo grupo con dos elementos es abeliano. En particular $(S_2, \circ)$ es abeliano.

15. Sean G un grupo y $a_i \in G$, $1 \leq i \leq n$. Entonces se verifica:

a) $(a_1 \cdots a_k)(a_{k+1} \cdots a_n) = (a_1 \cdots a_l)(a_{l+1} \cdots a_n)$, donde $1 < k < l < n$.

b) $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

16. Demostrad que:

a) $(S^1, \cdot)$ es subgrupo de $(\mathbb{C} \setminus \{0\}, \cdot)$.

b) $O_n(\mathbb{R})$ es subgrupo de $(GL_n(\mathbb{R}), \cdot)$.

c) $(\mathbb{Z}, +)$ es subgrupo de $(\mathbb{Q}, +)$.

17. Sea G un grupo y $a \in G$ un elemento de orden finito. Probad que:

a) Si $o(a) = pq$ con $\text{mcd}(p, q) = 1$, entonces existen dos únicos elementos $x, y \in G$ tales que $a = xy = yx$ y $o(x) = p$, $o(y) = q$.

b) Si $b \in G$ es tal que ab es un elemento de orden finito, probad que también lo es ba y, además, $o(ab) = o(ba)$.

c) Si $x \in G$, probad que el elemento $b = xax^{-1}$ tiene el mismo orden que a.

18. Sea G un grupo y H un subgrupo normal de G tal que $H \subseteq Z(G)$, siendo $Z(G) = \{a \in G : ax = xa, \forall x \in G\}$ el centro del grupo G. Probad que si G/H es cíclico, entonces G es abeliano.

Capítulo 2

Homomorfismos de grupos

En el estudio de las estructuras algebraicas, las aplicaciones entre objetos que respetan la estructura son un instrumento fundamental, ya que permiten establecer, de manera unívoca, representaciones para objetos diferentes pero de comportamiento idéntico.

2.1. Definiciones y propiedades

Definición 2.1.1 *Dados dos grupos G y G', diremos que una aplicación $f : G \longrightarrow G'$ es un homomorfismo de grupos si verifica que*

$$f(ab) = f(a)f(b) \qquad \text{para cada} \qquad a, b \in G.$$

Comunmente se dice también que f es un morfismo. Nosotros emplearemos indistintamente los dos términos.

Ejemplo 2.1.2 *1. Todo homomorfismo de espacios vectoriales es en particular un homomorfismo de grupos.*

2. Dados los grupos $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, la aplicación dada por

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^* \\ x &\longmapsto e^x \end{aligned}$$

es un homomomorfismo de grupos, ya que

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y).$$

3. Dados los grupos $(Aut(\mathbb{R}^2), \circ)$, $(Gl_2(\mathbb{R}), \cdot)$, la aplicación dada por

$$\begin{aligned} \phi : Aut(\mathbb{R}^2) &\longrightarrow Gl_2(\mathbb{R}) \\ f &\longmapsto M_B(f), \end{aligned}$$

donde $M_B(f)$ representa a la matriz asociada a f en una cierta base B, es un homomorfismo de grupos, ya que

$$\phi(f \circ g) = M_B(f \circ g) = M_B(f) \cdot M_B(g) = \phi(f) \cdot \phi(g).$$

4. *La aplicación*

$$\begin{array}{rcl} f : S^1 & \longrightarrow & SL_2(\mathbb{R}) \\ e^{i\theta} & \longmapsto & \begin{pmatrix} \cos\theta & \operatorname{sen}\theta \\ -\operatorname{sen}\theta & \cos\theta \end{pmatrix} \end{array}$$

es un morfismo de grupos.

Proposición 2.1.3 *Sean G y G' dos grupos, y sea $f : G \longrightarrow G'$ un homomorfismo de grupos. Entonces se verifica:*

1. $f(1) = 1$.
2. $f(a^{-1}) = f(a)^{-1}$ *para cada* $a \in G$.

DEMOSTRACIÓN.

(1) Se tiene que $f(1) = f(1 \cdot 1) = f(1)f(1)$, por tanto $f(1) = 1$.

(2) Se verifica que

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1) = 1.$$

De la misma forma demostramos que $f(a^{-1})f(a) = 1$. Por tanto, $f(a^{-1}) = f(a)^{-1}$ para cada $a \in G$.

■

2.2. Núcleo e Imagen de un homomorfismo

Con objeto de estudiar morfismos arbitrarios bajo el prisma de una descomposición canónica, necesitamos introducir ciertos subgrupos distinguidos asociados a dicho morfismo.

Definición 2.2.1 *Sean G y G' dos grupos y $f : G \longrightarrow G'$ un homomorfismo de grupos. Llamamos:*

1. *Núcleo de f, y lo denotamos por* $\ker(f)$, *al siguiente conjunto*

$$\ker(f) = \{x \in G : f(x) = 1\}.$$

2. *Imagen de f, y lo denotamos por* $\mathrm{Im}(f)$*, al siguiente conjunto*

$$\mathrm{Im}(f) = \{f(x) : x \in G\}.$$

Proposición 2.2.2 *Sean G y G' dos grupos, y sea $f : G \longrightarrow G'$ un homomorfismo de grupos. Entonces:*

1. $\ker(f)$ *es un subgrupo normal de G.*
2. $\mathrm{Im}(f)$ *es un subgrupo de G'.*

Demostración.

1. $\ker(f)$ es subgrupo normal de G. Vamos a verlo:
   - $\ker(f) \neq \emptyset$, ya que $1 \in \ker(f)$.
   - $\ker(f) \subseteq G$, por definición.
   - Sean $x, y \in \ker(f)$, entonces tendremos que
   $$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1 \cdot 1^{-1} = 1.$$
   Por tanto $xy^{-1} \in \ker(f)$.
   - $\ker(f)$ es un subgrupo normal de G, ya que para todo $a \in G$, se verifica $a^{-1}\ker(f)a \subseteq \ker(f)$. Vamos a verlo. Si $x \in a^{-1}\ker(f)a$, entonces $x = a^{-1}ya$ con $y \in \ker(f)$. Por tanto
   $$f(x) = f(a^{-1}ya) = f(a^{-1})f(y)f(a) = f(a)^{-1}f(y)f(a) = 1,$$
   luego $x \in \ker(f)$, y así $a^{-1}\ker(f)a \subseteq \ker(f)$.
2. $\mathrm{Im}(f)$ es subgrupo de G'. Vamos a verlo:
   - $\mathrm{Im}(f) \neq \emptyset$, ya que $1 = f(1) \in \mathrm{Im}(f)$.
   - $\mathrm{Im}(f) \subseteq G'$ por definición de $\mathrm{Im}(f)$.
   - Si $f(x_1), f(x_2) \in \mathrm{Im}(f)$, entonces
   $$f(x_1)f(x_2)^{-1} = f(x_1)f(x_2^{-1}) = f(x_1x_2^{-1}),$$
   donde $x_1x_2^{-1} \in G$. Así $f(x_1)f(x_2)^{-1} \in \mathrm{Im}(f)$, luego $\mathrm{Im}(f)$ es un subgrupo de G'.

■

Definición 2.2.3 *Dado $f : G \longrightarrow G'$ un homomorfismo de grupos, diremos que:*

1. *f es monomorfismo si f es inyectivo.*
2. *f es epimorfismo si f es sobreyectivo.*
3. *f es isomorfismo si f es biyectivo.*
4. *f es un endomorfismo si $G = G'$.*
5. *f es un automorfismo si f es un endomorfismo biyectivo.*

Ejemplos 2.2.4 1. *Si H es un subgrupo de G, la inclusión de H en G es un monomorfismo.*

2. *Si N es un subgrupo normal de G, la aplicación $\pi : G \longrightarrow G/H$ dada por $\pi(x) = xH$ es un epimorfismo que recibe el nombre de proyección canónica de G sobre G/H. Su núcleo es $\ker(\pi) = N$.*

3. *Dados dos grupos G y H, la aplicación $f : G \longrightarrow H$ dada por $f(a) = 1$ para cada $a \in G$ es un homomorfismo llamado homomorfismo trivial de G en H. Su núcleo es todo G. Si $H \neq \{1\}$, entonces f no es ni monomorfismo ni epimorfismo.*

4. *La aplicación $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ dada por $f(n) = 3n$ es un monomorfismo pero no es epimorfismo. De hecho, como veremos, todo endomorfismo de $\mathbb{Z}$ está definido por multiplicación por un elemento $a \in \mathbb{Z}$.*

5. *El morfismo del Ejemplo 2.1.2(3) es un isomorfismo.*

Nuestro primer objetivo es caracterizar monomorfismos, epimorfismos e isomorfismos en función del núcleo y la imagen.

Proposición 2.2.5 *Sean G y G' dos grupos y $f : G \longrightarrow G'$ un homomorfismo de grupos. Entonces se verifica:*

1. *f es monomorfismo $\iff \ker(f) = \{1\}$.*
2. *f es epimorfismo $\iff \mathrm{Im}(f) = G'$.*

DEMOSTRACIÓN.

(1) $\Longrightarrow$: Si $x \in \ker(f)$ entonces $f(x) = 1$. Por otro lado se verifica que $f(1) = 1$. Por tanto, $f(x) = f(1)$, y al ser f una aplicación inyectiva, tenemos que $x = 1$. Por tanto $\ker(f) = \{1\}$.

$\Longleftarrow$: Veamos que f es una aplicación inyectiva. Supongamos que $f(x) = f(y)$. Entonces $f(x)f(y)^{-1} = 1$, es decir $1 = f(x)f(y)^{-1} = f(xy^{-1})$, y así $xy^{-1} \in \ker(f)$. Como por hipótesis $\ker(f) = \{1\}$, entonces $xy^{-1} = 1$, y de ahí que $x = y$.

(2) Evidente.

■

A continuación caracterizaremos los isomorfismos en función de núcleo e imagen. Para ello necesitamos el siguiente resultado previo.

Lema 2.2.6 *Si $f : G \longrightarrow G'$ es un isomorfismo entre los grupos G y G', entonces $f^{-1} : G' \longrightarrow G$ es también un isomorfismo.*

DEMOSTRACIÓN. En efecto, como la inversa de toda aplicación biyectiva también lo es, nos bastará demostrar que f^{-1} es un homomorfismo de grupos. Sean $y_1, y_2 \in G'$ tales que $f^{-1}(y_1) = x_1$, $f^{-1}(y_2) = x_2$, es decir $f(x_1) = y_1$, $f(x_2) = y_2$. Como f es un homomorfismo, tendremos que

$$f(x_1x_2) = f(x_1)f(x_2) = y_1y_2$$

luego $x_1x_2 = f^{-1}(y_1y_2)$, de donde

$$f^{-1}(y_1y_2) = x_1x_2 = f^{-1}(y_1)f^{-1}(y_2).$$

Así podemos afirmar que f^{-1} es un homomorfismo de grupos.

■

Proposición 2.2.7 *Sea $f : G \to G'$ un morfismo de grupos. Entonces, f es isomorfismo si y sólo si es monomorfismo y epimorfismo.*

DEMOSTRACIÓN. Si f es isomorfismo, por el Lema 2.2.6, se tiene que la aplicación $g := f^{-1} : G' \to G$ es isomorfismo. Entonces,

$$gf = Id_G, \qquad fg = Id_{G'}.$$

Sea $x \in \ker(f)$. Entonces, $x = g(f(x)) = g(1) = 1$, de donde f es monomorfismo. Sea $y \in G'$. Entonces, $y = f(g(y))$ con $g(y) \in G$, por lo que f es epimorfismo.

Recíprocamente, si f es monomorfismo y epimorfismo, definimos

$$\begin{array}{rccl} g: & G' & \longrightarrow & G \\ & y & \longmapsto & x \text{ (tal que } f(x) = y) \end{array}$$

Como f es epimorfismo, g está definida para todo $y \in G'$.

Como f es monomorfismo, existe un único $x \in G$ tal que $f(x) = y$, por lo que la aplicación g está bien definida. Veamos que es morfismo de grupos. Sean $y, y' \in G'$ y sean $x = g(y)$, $x' = g(y')$, y $x'' = g(yy')$. Entonces, por definición de g, tenemos $f(x) = y$, $f(x') = y'$, $f(x'') = yy' = f(x)f(x') = f(xx')$. Como f es monomorfismo, tenemos $x'' = xx'$, de donde $g(yy') = g(y)g(y')$. Por tanto es morfismo de grupos, y claramente $gf = Id_G$, $fg = Id_H$.

■

Proposición 2.2.8 *Sea $f : G \longrightarrow G'$ un homomorfismo entre los grupos G y G'. Entonces:*

1. *Si H es un subgrupo de G entonces $f(H)$ es un subgrupo de G'.*
2. *Si H' es un subgrupo de G' entonces*
$$f^{-1}(H') = \{x \in G : f(x) \in H'\}$$
es un subgrupo de G.
3. *Si H' es un subgrupo normal de G' entonces $f^{-1}(H')$ es un subgrupo normal de G.*
4. *Si H es un subgrupo normal de G y f es un epimorfismo entonces $f(H)$ es un subgrupo normal de G'.*

DEMOSTRACIÓN.

(1) (a) Tenemos que $f(H) \neq \emptyset$ ya que $1 = f(1) \in f(H)$, al ser H un subgrupo de G. Por definición se verifica que $f(H) \subseteq G'$.

(b) Para cualesquiera y_1, $y_2 \in f(H)$ existen x_1, $x_2 \in H$ tales que $f(x_1) = y_1$ y $f(x_2) = y_2$. Como f es un homomorfismo de grupos,
$$y_1 y_2^{-1} = f(x_1)f(x_2)^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1})$$
donde $x_1 x_2^{-1} \in H$, por ser H un subgrupo de G. Por tanto, $y_1 y_2^{-1} \in f(H)$.

(2) (a) $f^{-1}(H') \neq \emptyset$, ya que $f(1) = 1 \in H'$, al ser H' un subgrupo. Por tanto $1 \in f^{-1}(H')$.

(b) Si $x_1, x_2 \in f^{-1}(H')$, entonces se verifica $f(x_1), f(x_2) \in H'$, y al ser H' un subgrupo,
$$f(x_1 x_2^{-1}) = f(x_1)f(x_2^{-1}) = f(x_1)f(x_2)^{-1} \in H'.$$
Así $x_1 x_2^{-1} \in f^{-1}(H')$.

(3) Veamos que $f^{-1}(H')$ es un subgrupo normal de G. Sean $x_1, x_2 \in G$ tales que $x_1 x_2 \in f^{-1}(H')$. Entonces $f(x_1 x_2) \in H'$. Por tanto,
$$f(x_1)f(x_2) = f(x_1 x_2) \in H',$$
y al ser H' un subgrupo normal de G', tendremos que
$$f(x_2 x_1) = f(x_2)f(x_1) \in H',$$
y de ahí que $x_2 x_1 \in f^{-1}(H')$. Por tanto, $f^{-1}(H')$ es un subgrupo normal de G.

(4) Veamos que para cualquier $y \in G'$ se tiene

$$y^{-1}f(H)y \subseteq f(H).$$

Si $z \in y^{-1}f(H)y$, entonces $z = y^{-1}f(h)y$ con $h \in H$. Por otro lado, como f es una aplicación sobreyectiva, existe $x \in G$ tal que $y = f(x)$. Así tenemos que

$$z = f(x)^{-1}f(h)f(x) = f(x^{-1}hx).$$

Pero H es un subgrupo normal en G, de donde $x^{-1}hx \in H$, y de ahí que $z \in f(H)$. Así queda demostrado que $f(H)$ es un subgrupo normal en G'.

■

Observación 2.2.9 *1. Como* $\ker(f) = f^{-1}(\{1\})$, *y* $\{1\}$ *es un subgrupo normal de* G', *se tiene de nuevo que* $\ker(f)$ *es un subgrupo normal de* G.

2. La afirmación de Proposición 2.2.8(4) falla cuando se pierde la exhaustividad del morfismo. Por ejemplo, como veremos en el Teorema 2.4.3, el subgrupo de S_3 *generado por* $(1,2)$ *(la permutación que cambia* 1 *por* 2, 2 *por* 1 *y deja fijo* 3*) es isomorfo a* $\mathbb{Z}/2\mathbb{Z}$. *Sin embargo* $\langle(1,2)\rangle$ *no es normal, ya que* $(1,2,3)(1,2)(1,2,3)^{-1} = (2,3)$. *Por tanto, el monomorfismo* $f : \mathbb{Z}/2\mathbb{Z} \longrightarrow S_3$, *definido por* $f(\overline{1}) = (1,2)$, *envía un subgrupo normal a un subgrupo que no lo es.*

El orden de un elemento también se ve afectado por los morfismos de grupo como se demuestra en la siguiente proposición.

Proposición 2.2.10 *Sea* $f : G \longrightarrow G'$ *un homomorfismo entre los grupos* G *y* G', *y sea* $x \in G$ *un elemento de orden* m. *Entonces se verifica:*

1. $o(f(x))$ *divide a* m.

2. Si f *es inyectiva, entonces* $o(f(x)) = m$.

DEMOSTRACIÓN.

(1) Si x es un elemento de orden m, entonces se verifica que $x^m = 1$. Por tanto

$$f(x)^m = f(x^m) = f(1) = 1,$$

luego $o(f(x))$ divide a m.

(2) Por el apartado anterior se tiene $o(f(x))$ divide a m. Si $o(f(x)) = k$, entonces $f(x)^k = 1$, luego $f(x^k) = 1$. Así, $x^k \in \ker(f)$. Pero al ser f una aplicación inyectiva, por la Proposición 2.2.5(1), tenemos que $x^k = 1$, luego m divide a k, o lo que es lo mismo, m divide a $o(f(x))$. Así $o(f(x)) = m$.

■

Asimismo se tiene un buen comportamiento de los morfismos respecto de la composición, allí donde ésta tiene sentido.

Proposición 2.2.11 *Sean $f : G \longrightarrow G'$ y $g : G' \longrightarrow G''$ dos homomorfismos entre los grupos G, G' y G''. Entonces también lo es*

$$g \circ f : G \longrightarrow G''.$$

DEMOSTRACIÓN. Dados $x, y \in G$, se tiene que

$$(g \circ f)(xy) = g[f(xy)] = g[f(x)f(y)] = g[f(x)]g[f(y)] = (g \circ f)(x)(g \circ f)(y).$$

■

Notación 2.2.12 *Denotaremos por:*

- *$Hom(G, G')$ al conjunto de todos los homomorfismos de G en G'.*
- *$End(G)$ al conjunto de todos los endomorfismos en G.*
- *$Aut(G)$ al conjunto de todos los automorfismos en G.*

En particular, del Lema 2.2.6 y Proposición 2.2.11 se desprende que $Aut(G)$ es un grupo con la operación composición, y la identidad como elemento neutro.

Definición 2.2.13 *Diremos que los grupos G y G' son isomorfos si existe un isomorfismo $f : G \longrightarrow G'$. En tal caso, lo denotaremos por $G \cong G'$.*

Dos grupos isomorfos tienen las "mismas propiedades" como grupos. En la siguiente proposición presentaremos varios ejemplos de este hecho.

Proposición 2.2.14 *Sean G y G' dos grupos isomorfos. Entonces se verifica:*

1. *G es abeliano si y sólo si G' es abeliano.*
2. *G es cíclico si y sólo si G' es cíclico.*

DEMOSTRACIÓN.

(1) Si G y G' son isomorfos, entonces existirá un isomorfismo $f : G \longrightarrow G'$. Si $y_1, y_2 \in G'$, como f es aplicación sobreyectiva, existen $x_1, x_2 \in G$ tales que

$$y_1 = f(x_1), \qquad y_2 = f(x_2).$$

Así, al ser f un homomorfismo y G abeliano tendremos:

$$y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2) = f(x_2 x_1) = f(x_2)f(x_2) = y_2 y_1.$$

La implicación contraria es consecuencia de que f^{-1} es isomorfismo si f lo es.

(2) Si G es cíclico, entonces tendremos $G = \langle a \rangle$ con $a \in G$. Vamos a probar que $G' = \langle f(a) \rangle$. Si $y \in G'$ entonces, como f es una aplicación sobreyectiva, existe $x \in G$ tal que $f(x) = y$. Pero si $x \in G = \langle a \rangle$, existirá un entero $k \in \mathbb{Z}$ tal que $x = a^k$. Así

$$y = f(x) = f(a^k) = f(a)^k \in \langle f(a) \rangle,$$

luego $G' \subseteq \langle f(a) \rangle$. Como siempre se verifica que $\langle f(a) \rangle \subseteq G'$, entonces tendremos que $G' = \langle f(a) \rangle$. La implicación contraria se demuestra aplicando este resultado a f^{-1}, que es también un isomorfismo.

■

Como aplicación de la proposición anterior, podemos afirmar que S_3 no puede ser isomorfo a $\mathbb{Z}_6$, ya que éste es abeliano mientras que el primero no lo es. Por lo tanto, el orden de un subgrupo no clasifica a éste salvo isomorfismo, aunque grupos isomorfos tiene necesariamente la misma cardinalidad.

La siguiente proposición justifica el hecho de que al grupo de las permutaciones de un conjunto X de n elementos en sí mismo, le llamemos S_n.

Proposición 2.2.15 *Sean X, Y dos conjuntos no vacíos con la misma cardinalidad. Entonces los grupos $(S(X), \circ)$ y $(S(Y), \circ)$ son isomorfos.*

DEMOSTRACIÓN. Como X e Y tienen la misma cardinalidad, podemos establecer una biyección $f : X \longrightarrow Y$. Consideremos la siguiente aplicación:

$$\begin{aligned} \phi : S(X) &\longrightarrow S(Y) \\ g &\longrightarrow f \circ g \circ f^{-1}. \end{aligned}$$

Vamos a probar que ϕ es un isomorfismo.

- ϕ es homomorfismo ya que

$$\phi(g \circ h) = f \circ (g \circ h) \circ f^{-1} = (f \circ g \circ f^{-1}) \circ (f \circ h \circ f^{-1}) = \phi(g) \circ \phi(h).$$

- ϕ es inyectiva ya que si $\phi(g) = \phi(h)$, entonces $f \circ g \circ f^{-1} = f \circ h \circ f^{-1}$, luego $g = h$.

- ϕ es sobreyectiva ya que para cada $h \in S(Y)$, existe $g = f^{-1} \circ h \circ f \in S(X)$ tal que $\phi(g) = h$.

■

Ejemplo 2.2.16 *Vamos a calcular todos los homomorfismos $f : \mathbb{Z} \longrightarrow \mathbb{Z}$. Supongamos que f sea un endomorfismo en $\mathbb{Z}$. En particular*

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ 1 & \longmapsto & a. \end{array}$$

Entonces dado $n \in \mathbb{Z}$, tendremos que:

- *Si $n > 0$,*

$$f(n) = f(\overbrace{1 + \cdots + 1}^{(n)}) = \overbrace{f(1) + \cdots + f(1)}^{(n)} = f(1)n = an.$$

- *Si $n = 0$, entonces se verificará $f(0) = 0$ ya que 0 es el elemento neutro en el grupo aditivo de los números enteros.*

- *Si $n < 0$, consideremos $m = -n > 0$ y*

$$f(n) = f(-m) = -f(m) = -(ma) = a(-m) = an.$$

Recíprocamente, la aplicación $f(n) = na$ es un homomorfismo ya que

$$f(n + m) = a(n + m) = an + am = f(n) + f(m).$$

Por tanto, los homomorfismos $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ son las aplicaciones

$$\begin{array}{rcl} f_a : \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & an \end{array}$$

para cada $a \in \mathbb{Z}$.

2.3. Factorización canónica de un homomorfismo

Finalmente, procedemos a establecer la manera en que cualquier morfismo de grupos factoriza, de manera canónica, a través de un epimorfismo y un monomorfismo. Para ello, presentaremos en primer lugar un resultado más general.

Proposición 2.3.1 *Sea $f : G \longrightarrow G'$ un homomorfismo de grupos, y sea H un subgrupo normal de G. Entonces son equivalentes:*

1. *H es un subgrupo de* $\ker(f)$.
2. *Existe un único homomorfismo $\overline{f} : G/H \longrightarrow G'$ tal que $\overline{f} \circ \pi = f$.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2) : Sea la aplicación $\overline{f} : G/H \longrightarrow G'$ definida por $\overline{f}(aH) = f(a)$. Veamos que:

- $\overline{f}$ está bien definida, ya que si $aH = bH$ entonces $a^{-1}b \in H$, siendo H un subgrupo de $\ker(f)$. Por tanto, $f(a^{-1}b) = 1$, y al ser f un homomorfismo, $f(a) = f(b)$ con lo cual $\overline{f}(aH) = \overline{f}(bH)$.
- $\overline{f}$ es homomorfismo de grupos, ya que $\overline{f}((aH)(bH)) = \overline{f}(abH) = f(ab) = f(a)f(b) = \overline{f}(aH)\overline{f}(bH)$.
- $\overline{f} \circ \pi = f$, ya que para todo $a \in G$, se tiene
$$\left(\overline{f} \circ \pi\right)(a) = \overline{f}(aH) = f(a).$$
- $\overline{f}$ es único, ya que supongamos que existe $g : G/H \longrightarrow G'$ tal que $g \circ \pi = f$. Entonces se tiene, para todo $aH \in G/H$:
$$g(aH) = g(\pi(a)) = (g \circ \pi)(a) = f(a) = \left(\overline{f} \circ \pi\right)(a) = f(aH).$$

$2 \Longrightarrow 1$: Sea $x \in H$. Entonces $xH = H$, por tanto, al ser $\overline{f}$ un homomorfismo de grupos, $\overline{f}(xH) = 1$. Pero $1 = \overline{f}(xH) = (\overline{f} \circ \pi)(x) = f(x)$, de donde $x \in \ker(f)$.

■

Proposición 2.3.2 (Factorización canónica de un homomorfismo) *Sea $f : G \longrightarrow G'$ un homomorfismo entre los grupos G y G'. Entonces existe un único isomorfismo*
$$\overline{f} : G/\ker(f) \longrightarrow \mathrm{Im}(f)$$
que hace conmutativo el siguiente diagrama,
$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker(f) & \xrightarrow{\overline{f}} & \mathrm{Im}(f) \end{array}$$

DEMOSTRACIÓN. Sea el monomorfismo

$$\begin{aligned} i : Im(f) &\longrightarrow G' \\ f(x) &\longmapsto f(x). \end{aligned}$$

Consideremos el homomorfismo de grupos dado por $f_1 : G \longrightarrow \mathrm{Im}(f)$, y observemos que $i \circ f_1 = f$. Como $\ker(f)$ es un subgrupo normal de G, por la Proposición 2.3.1, existe un único homomorfismo

$$\begin{aligned} \overline{f} : G/\ker(f) &\longrightarrow \mathrm{Im}(f) \\ x(\ker(f)) &\longmapsto f(x) \end{aligned}$$

tal que $\overline{f} \circ \pi = f_1$. Veamos que $\overline{f}$ es un isomorfismo:

- $\overline{f}$ es monomorfismo. Si $x(\ker(f)) \in \ker(\overline{f})$, tendremos que

$$1 = \overline{f}(x(\ker(f))) = f(x),$$

  luego $\ker(\overline{f})$ es la clase de $\ker(f)$, es decir, $\overline{1}$.

- $\overline{f}$ es epimorfismo, ya que $\mathrm{Im}(f) = \mathrm{Im}(\overline{f})$.

Por tanto $\overline{f}$ es un isomorfismo. Por último afirmamos que el diagrama es conmutativo, ya que

$$(i \circ \overline{f} \circ \pi) = i \circ (\overline{f} \circ \pi) = i \circ f_1 = f.$$

■

2.4. Teoremas de Isomorfía

La escisión canónica establece métodos para representar ciertos grupos mediante imágenes isomorfas. Son los llamados Teoremas de Isomorfía.

Corolario 2.4.1 (Primer Teorema de Isomorfía) *Si $f : G \longrightarrow G'$ es un homomorfismo entre los grupos G y G', entonces se verifica:*

$$G/\ker(f) \cong \mathrm{Im}(f).$$

DEMOSTRACIÓN. Es consecuencia inmediata de la Proposición 2.3.2, al afirmar la existencia del isomorfismo

$$\begin{aligned} \overline{f} : G/\ker(f) &\longrightarrow \mathrm{Im}(f) \\ x(\ker(f)) &\longmapsto f(x). \end{aligned}$$

■

Ejemplo 2.4.2 *La aplicación* $f : \mathbb{C}^* \longrightarrow \mathbb{R}^+ \setminus \{0\}$, *definida asignando a cada complejo no nulo su norma, es un epimorfismo. Dado que su núcleo es* $\ker(f) = S^1$, *concluimos por el Primer Teorema de Isomorfía que* $\mathbb{C}^*/S^1 \cong \mathbb{R}^+ \setminus \{0\}$.

Utilizando el Primer Teorema de Isomorfía, podemos establecer una clasificación para los grupos cíclicos.

Teorema 2.4.3 (Teorema de clasificación de los grupos cíclicos)

1. *Si* G *es un grupo cíclico infinito, entonces* G *es isomorfo al grupo* $(\mathbb{Z}, +)$.
2. *Si* G *es un grupo cíclico finito, entonces* G *es isomorfo al grupo* $(\mathbb{Z}/n\mathbb{Z}, +)$ *para algún* $n \in \mathbb{N}$.

DEMOSTRACIÓN. Si G es un grupo cíclico, entonces existe $a \in G$ tal que $G = \langle a \rangle$. Así tiene sentido considerar la siguiente aplicación:

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow G \\ k &\longmapsto a^k. \end{aligned}$$

Veamos que f es un epimorfismo.

- f es homomorfismo ya que $f(k_1 + k_2) = a^{k_1+k_2} = f(k_1)f(k_2)$.
- f es sobreyectiva, ya que cada elemento $b \in G = \langle a \rangle$ es de la forma $b = a^k$, para algún $k \in \mathbb{Z}$, y de ahí

$$b = a^k = f(k), \text{ para algún } k \in \mathbb{Z}.$$

Aplicando el Primer Teorema de Isomorfía, tendremos:

$$\mathbb{Z}/\ker(f) \cong G.$$

Vamos a estudiar el conjunto $\ker(f)$. Pueden darse dos situaciones:

(1) Si $\ker(f) = \{0\}$, entonces $\mathbb{Z} \cong G$.

(2) Si Si $\ker(f) \neq \{0\}$, entonces existe un natural n tal que $\ker(f) = n\mathbb{Z}$. Entonces $\mathbb{Z}/n\mathbb{Z} \cong G$. En particular, $o(G) = n$.

■

Anteriormente habíamos demostrado que $\mathbb{Z}$ y $\mathbb{Z}/m\mathbb{Z}$ son grupos cíclicos, y con este teorema podemos afirmar que $\mathbb{Z}$ y $\mathbb{Z}/m\mathbb{Z}$ son los únicos grupos cíclicos que existen, salvo isomorfismo.

Corolario 2.4.4 *Sea* $f : G \longrightarrow G'$ *un homomorfismo sobreyectivo entre los grupos* G *y* G'. *Entonces:*

1. $G/\ker(f)$ *es isomorfo a* G'.

2. *Existe una correspondencia biyectiva entre los subgrupos de* G' *y los subgrupos de* G *que contienen a* $\ker(f)$.

A continuación vamos a dar la solución de algunos ejemplos de grupos cocientes que presentamos anteriormente

Ejemplo 2.4.5 *La aplicación*

$$\begin{aligned} f : (GL_2(\mathbb{R}), \cdot) &\longrightarrow (\mathbb{R}^*, .) \\ A &\longmapsto \det(A) \end{aligned}$$

es un epimorfismo. Si $A \in \ker(f)$ *entonces se verifica que* $\det(A) = 1$, *por tanto,* $\ker(f) = SL_2(\mathbb{R})$ *y de ahí que* $GL_2(\mathbb{R})/SL_2(\mathbb{R}) \cong \mathbb{R}^*$.

Ejemplo 2.4.6 *Dado un entero positivo* n *se define* $f_n : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +)$ *mediante* $f_n(z) = [z]_n$, *donde* $[z]_n$ *representa la clase de* z *módulo* n. *Entonces se verifica que* f_n *es un homomorfismo sobreyectivo. Vamos a calcular el* $\ker(f)$,

$$\ker(f) = \{z \in \mathbb{Z} : f_n(z) = [0]_m\} = \{z \in \mathbb{Z} : z \equiv 0(\text{mód}\, n)\} = n\mathbb{Z}.$$

Así aplicando el Primer Teorema de Isomorfía tendremos que,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

Ejemplo 2.4.7 *Dados dos números enteros positivos* n *y* m, *definimos*

$$\begin{aligned} f : (n\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}_m, +) \\ nz &\longmapsto [z]_m, \end{aligned}$$

donde $[z]_m$ *representa la clase de* z *módulo* m. *Se verifica que* f *es un homomorfismo sobreyectivo. Vamos a calcular el núcleo,*

$$\ker(f) = \{nz \in n\mathbb{Z} : f(nz) = [0]_m\} = \{nz \in n\mathbb{Z} : [z]_n = [0]_m\} =$$

$$= \{nz \in n\mathbb{Z} : z \equiv 0(\text{mód}\, m)\} = \{nz \in n\mathbb{Z} : z = km,\ k \in \mathbb{Z}\} =$$

$$= \{knm : k \in \mathbb{Z}\} = nm\mathbb{Z}.$$

Por tanto, $n\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}_m$.

Otra aplicación del Primer Teorema de Isomorfía es el Teorema Chino de los Restos

Teorema 2.4.8 (Teorema Chino de los Restos) *Sean $d_1, \ldots, d_t$ números enteros no nulos, coprimos dos a dos. Entonces*

$$\mathbb{Z}/(d_1 \cdots d_t)\mathbb{Z} \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z}).$$

DEMOSTRACIÓN. Consideremos la aplicación

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z}) \\ m &\longmapsto (m + d_1\mathbb{Z}, \cdots, m + d_t\mathbb{Z}). \end{aligned}$$

Claramente ϕ es un homomorfismo de grupos. Su núcleo viene dado por

$$\ker(\phi) = \{m \in \mathbb{Z} : \ d_i | m, \ 1 \leq i \leq t\}.$$

Como $\text{mcd}(d_i, d_j) = 1$ para $i \neq j$, tenemos que $\ker(\phi) = (d_1 \cdots d_t)\mathbb{Z}$.
Así $\mathbb{Z}/(d_1 \cdots d_t)\mathbb{Z}$ es isomorfo a un subgrupo de $(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z})$, pero

$$\text{card}\,(\mathbb{Z}/(d_1 \cdots d_t)\mathbb{Z}) = \text{card}\,(\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}),$$

de donde

$$\mathbb{Z}/(d_1 \cdots d_t)\mathbb{Z} \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z}).$$

■

Proposición 2.4.9 *Sea G un grupo, y sean H y K subgrupos normales de G tales que $H \cap K = \{1\}$. Entonces $HK \cong H \times K$.*

DEMOSTRACIÓN. Sin pérdida de generalidad, podemos suponer $G = HK$. Definimos

$$\begin{aligned} f : H \times K &\longrightarrow HK \\ (h, k) &\longmapsto hk. \end{aligned}$$

Como $H \cap K = \{1\}$, entonces $hk = kh$, para todo $h \in H$ y para todo $k \in K$. Por tanto, f es un morfismo. De forma clara se verifica que f es epimorfismo. Su núcleo viene dado por

$$\ker(f) = \{(h, k) : \ hk = 1\}.$$

Como $H \cap K = \{1\}$, se tiene que $\ker(f) = \{(1, 1)\}$. De todo lo anterior podemos afirmar que $H \times K \cong HK$.

■

Teorema 2.4.10 (Segundo Teorema de Isomorfía)
Sean N y H subgrupos normales de un grupo G, tales que $N \subseteq H$. Entonces se verifica que:

1. *H/N es subgrupo normal de G/N.*
2. *$(G/N)/(H/N) \cong G/H$.*

DEMOSTRACIÓN. Vamos a demostrar a la vez los dos apartados. Consideremos la aplicación

$$\begin{aligned} f : G/N &\longrightarrow G/H \\ aN &\longmapsto aH. \end{aligned}$$

Se verifica que:

- f está bien definida, ya que si $aN = bN$, se tiene que $a^{-1}b \in N \subseteq H$. Por tanto $aH = bH$, es decir $f(aN) = f(bN)$.
- f es un homomorfismo ya que si aN, $bN \in G/N$, entonces

$$f[(aN)(bN)] = f[(ab)N] = (ab)H = (aH)(bH) = f(aN)f(bN).$$

- f es sobreyectiva, ya que para cada $aH \in G/H$, existe $aN \in G/N$ tal que $f(aN) = aH$.
- Vamos a calcular $\ker(f)$. Si $aN \in \ker(f)$, entonces $f(aN) = aH = H$, esto es, $a \in H$, es decir

$$\ker(f) = \{aN \in G/N : a \in H\} = H/N.$$

Aplicando el Primer Teorema de Isomorfía, tenemos

$$(G/N)/(H/N) \cong G/H.$$

■

Observemos que el Segundo Teorema de Isomorfía implica que, en una situación en la que trabajemos con cocientes iterados, no es necesario arrastrar clases de clases de equivalencia.

Teorema 2.4.11 (Tercer Teorema de Isomorfía).
Sean H y N subgrupos de un grupo G, y N subgrupo normal de G. Entonces:

1. *$H \cap N$ es subgrupo normal de H.*
2. *HN es subgrupo de G.*
3. *N es subgrupo normal de HN.*
4. *$(HN)/N \cong H/(H \cap N)$*

DEMOSTRACIÓN.

(1) Sean $a, b \in H$ tales que $ab \in H \cap N$. Veremos que $ba \in H \cap N$.
Si $ab \in H \cap N$, entonces $ab \in N$, con $a, b \in G$. Pero al ser N subgrupo normal de G, entonces $ba \in N$. Por otra parte, si $a, b \in H$, y H es un subgrupo, tendremos que $ba \in H$ y de ahí afirmamos que

$$ba \in H \cap N.$$

(2) Para ver que HN es subgrupo de G, demostraremos que $HN = NH$.
Si $x \in HN$, existen $h \in H$ y $n \in N$ tales que $x = hn$. En particular $x \in hN$, pero al ser N subgrupo normal de G, tenemos que $hN = Nh$. Así,

$$x \in hN = Nh \subseteq NH,$$

de donde $HN \subseteq NH$. De la misma forma se demuestra que $NH \subseteq HN$. Por la Proposición 1.2.21, NH es subgrupo de G.

(3) Sabemos que $N \subseteq HN$. Por tanto, como N es un subgrupo normal en G, claramente N sea un subgrupo normal de NH.

(4) Consideramos la aplicación dada por

$$\begin{aligned} f : H &\longrightarrow (HN)/N \\ h &\longmapsto hN. \end{aligned}$$

Se verifica que:

- f es homomorfismo, ya que dados $h_1 h_2 \in H$, se tiene

$$f(h_1 h_2) = (h_1 h_2)N = (h_1 N)(h_2 N) = f(h_1) f(h_2).$$

- f es sobreyectiva, ya que para todo $xN \in (HN)/N$, se tiene que

$$x = hn, \text{ con } h \in H,\ n \in N.$$

Entonces $x^{-1}h = n^{-1} \in N$, luego $xN = hN = f(h)$. Así para todo $xN \in (HN)/N$, existe $h \in H$, tal que $f(h) = xH$.

- $\ker(f) = H \cap N$, ya que si $x \in \ker(f)$, tenemos que $f(x) = xN = N$, de donde $x \in N$. Así $\ker(f) \subseteq N$. Pero $\ker(f)$ es un subgrupo de H, de donde $\ker(f) \subseteq H \cap N$. Recíprocamente, si $x \in H \cap N$, en particular $x \in N$ y por tanto $f(x) = xN = N$, lo que es equivalente a afirmar que $x \in \ker(f)$. Así $N \cap H \subseteq \ker(f)$. Por tanto $\ker(f) = H \cap N$.

Así aplicando el Primer Teorema de Isomorfía, tenemos que

$$(HN)/N \cong H/(H \cap N).$$

■

2.5. Ejercicios

1. Decid cuáles de las aplicaciones siguientes son homomorfismos de grupos, indicando en cada caso si la aplicación es inyectiva o suprayectiva:

   a) $f : \mathbb{Z} \longrightarrow \mathbb{Q}^*$ definida por $f(x) = \frac{1}{2^x}$.

   b) $f : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ definida por $f(x) = x^3$.

   c) $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ definida por $f(x) = \ln(x)$ ($\mathbb{R}_+^*$ es el grupo multiplicativo de los números reales estrictamente positivos.)

2. Sea $f : (\mathbb{R}, +) \longrightarrow (GL_2(\mathbb{R}), \cdot)$ la aplicación dada por

$$f(x) = \begin{pmatrix} \cos x & \operatorname{sen} x \\ -\operatorname{sen} x & \cos x \end{pmatrix}.$$

   Demostrad que f es un homomorfismo y calculad su núcleo.

3. Designemos por $\mathbb{Q}_+^*, \mathbb{R}_+^*$ los grupos multiplicativos de los números (racionales o reales) estrictamente positivos. Sean $U = \{z \in \mathbb{C} : |z| = 1\}$ y $C_2 = \{1, -1\}$. Probad que:

   a) $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

   b) $\mathbb{C}^*/\mathbb{R}_+^* \cong U$.

   c) $\mathbb{C}^*/U \cong \mathbb{R}_+^* \cong \mathbb{R}^*/C_2$.

   d) $\mathbb{R}^*/\mathbb{R}_+^* \cong C_2 \cong \mathbb{Q}^*/\mathbb{Q}_+^*$.

   e) $\mathbb{Q}^*/C_2 \cong \mathbb{Q}_+^*$.

4. Sean n y m enteros positivos. Probad que:

   a) $Hom(\mathbb{Z}, \mathbb{Z}) = \{f_a : (a \in \mathbb{Z}) \wedge (f_a(x) = xa; \forall x \in \mathbb{Z})\}$.

   b) $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \{0\}$.

   c) $Hom(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) =$
   $= \{f_a : (a \in \{0, 1, \ldots, n-1\}) \wedge (f_a(x) = xa + n\mathbb{Z}; \forall x \in \mathbb{Z})\}$.

   d) $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \left\{f_a(x + m\mathbb{Z}) = ax + n\mathbb{Z},\ a = \frac{n}{d}a',\ \forall x \in \mathbb{Z})\right\}$, siendo $d = \operatorname{mcd}(n, m)$ y $a' \in \{0, 1, \ldots, d-1\}$.

5. Sean $m, n \in \mathbb{Z}^+ \setminus \{0\}$.

   a) Probad que si existe un homomorfismo inyectivo de $\mathbb{Z}/m\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$ entonces $m \mid n$.

   b) Si $m \mid n$ y para cada $a' \in \{0, 1, \ldots, m-1\}$ consideramos $f_a \in Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ definido por $f_a(x + m\mathbb{Z}) = \frac{n}{m}xa' + n\mathbb{Z}$. Probad que:

$$f_a \text{ es inyectivo} \iff \text{mcd}(a', m) = 1.$$

6. Sean $m, n \in \mathbb{Z}^+ \setminus \{0\}$ y $d = \text{mcd}(m, n)$.

   a) Probad que si existe un homomorfismo sobreyectivo de $\mathbb{Z}/m\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$ entonces $n \mid m$.

   b) Si $n \mid m$ y para cada $a \in \{0, 1, \ldots, d-1\}$ consideramos $f_a \in Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ definido por $f_a(x + m\mathbb{Z}) = ax + n\mathbb{Z}$.
   Probad que: f_a es sobreyectivo $\iff$ $\text{mcd}(a, n) = 1$.

7. Probad que:

   a) La aplicación $\phi : Gl_n(K) \longrightarrow K^*$ definida por $\phi(A) = \det(A)$, es un homomorfismo de grupos (siendo $K = \mathbb{R}, \mathbb{Q}, \mathbb{C}$).

   b) $Sl_n(\mathbb{Q}) = \{A \in M_n(\mathbb{Q}) : \det(A) = 1\}$ es un subgrupo normal de $Gl_n(\mathbb{Q})$.

   c) $H = \{A \in Gl_n(\mathbb{R}) : |\det(A)| = 1\}$ es un subgrupo normal de $Gl_n(\mathbb{R})$.

   d) $Gl_n(\mathbb{R})/H \cong \mathbb{R}^+ - \{0\}$.

   e) $K = \{A \in Gl_n(\mathbb{R}) : \det(A) \in \mathbb{R}^+ - \{0\}\}$ es un subgrupo normal de $Gl_n(\mathbb{C})$.

   f) $Gl_n(\mathbb{C})/\mathbb{C}$ es isomorfo a $\{z \in \mathbb{C} : |z| = 1\}$.

8. Sea f la siguiente aplicación

$$\begin{aligned} f : \mathbb{R}^* &\longrightarrow \mathbb{R}^* \\ x &\longrightarrow x^2. \end{aligned}$$

   a) Demostrad que esta aplicación es un homomorfismo de grupos.

   b) Hallad $\ker(f)$ e $\text{Im}(f)$.

   c) Hallad el grupo cociente $\mathbb{R}^*/\ker(f)$ y la descomposición de f.

9. Demostrad que los grupos:

   a) $(\mathbb{R}, +)$ y $(\mathbb{R}_+^*, \cdot)$ son isomorfos.

   b) $(\mathbb{Z}, +)$ no es isomorfo a $(\mathbb{Q}, +)$.

   c) $(\mathbb{Z}, +)$ no es isomorfo a $(\mathbb{Q}^*, \cdot)$.

   d) $(\mathbb{Q}, +)$ no es isomorfo a $(\mathbb{Q}^*, \cdot)$

10. Sea G un grupo abeliano y

$$\begin{aligned} f : G &\longrightarrow G \\ x &\longrightarrow x^2. \end{aligned}$$

    Demostrad que:

a) f es homomorfismo $\Longleftrightarrow$ G es abeliano.

b) f es inyectiva $\Longleftrightarrow$ $o(G)$ es impar.

11. Sea G un grupo y N un subgrupo normal de G de orden n tal que el orden de N es primo con su índice. Demostrad que N es el único subgrupo de orden n de G.

12. Sea G un grupo. Para cada $a \in G$ consideramos la aplicación σ_a de G en G definida por $\sigma_a(x) = axa^{-1}$. Probad que:

a) σ_a es un automorfismo en G, denominado automorfismo interno.

b) $Aut(G)$ es un subgrupo de $Biy(G)$, en particular $Aut(G)$ es un grupo.

c) $Int(G)$ es un subgrupo de $Aut(G)$, siendo

$$Int(G) = \{\sigma_a : a \in G\}.$$

d) La aplicación $F : G \longrightarrow Aut(G)$ definida por $F(a) = \sigma_a$ es un homomorfismo de grupos. Hallad $\ker(F)$ e $\mathrm{Im}(F)$.

e) $G/Z(G) \cong Int(G)$.

13. Sea G un grupo y N un subgrupo normal de G de orden n tal que el orden de N es primo con su índice. Demostrad que N es el único subgrupo de orden n de G.

Capítulo 3

Grupos Abelianos Finitamente Generados

Este capítulo se centra en estudiar la clase de grupos abelianos con un número finito de generadores. El objetivo es obtener teoremas de estructura y clasificación para esta clase particular. Usaremos una argumentación basada en técnicas del Álgebra Lineal, que tomamos prestada de [7], y que nos parece más intuitiva.

3.1. Torsión en un grupo

Definición 3.1.1 *Sea G un grupo. Consideramos el conjunto*

$$T(G) = \{x \in G : o(x) \text{ es finito}\}.$$

Decimos que G tiene torsión si $T(G) \neq \{1\}$. Decimos que G es libre de torsión en caso contrario.

Observaciones 3.1.2 *1. Si G es abeliano, entonces $T(G)$ es un subgrupo de G:*

- *$T(G) \neq \emptyset$, pues $1 \in T(G)$ ya que $o(1) = 1$.*
- *Sean $x, y \in T(G)$. Como G es abeliano, por la Proposición 1.3.6, $o(xy^{-1})$ divide al mínimo común múltiplo de $o(x)$ y de $o(y^{-1})$, donde $o(y^{-1}) = o(y)$. Así $xy^{-1} \in T(G)$.*

Decimos que $T(G)$ es el subgrupo de torsión de G.

2. En general, si G no es abeliano, $T(G)$ no es subgrupo de G. Consideremos, por ejemplo, el grupo $G = GL_2(\mathbb{R})$ y sean

$$x = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}.$$

Evidentemente

$$x^2 = y^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1,$$

luego $x, y \in T(G)$. *Sin embargo* $xy \notin T(G)$, *pues se puede probar, por inducción, que para cada* $n \in \mathbb{N}$

$$(xy)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq 1.$$

3. *Sea* G *un grupo abeliano y* $T = T(G)$. *Entonces el cociente* G/T *no tiene torsión. Esto es porque, si* $o(xT) = n$, *resulta que* $(xT)^n = T$, *es decir* $x^nT = T$. *Entonces* $x^n \in T$, *es decir* $o(x^n)$ *es finito. o lo que es lo mismo* $(x^n)^m = 1$ *para cierto entero positivo* m, *y de aquí* $x^{nm} = 1$, *luego* $x \in T$ *y así* $xT = T$.

4. *El grupo* $G = \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{(r)}$ *es libre de torsión. Esto es obvio, ya que, si* $x \in G \setminus \{1\}$ *siendo* $x = (x_1, \cdots, x_r)$, *entonces* $x_i \neq 0$ *para algún* i, *con* $1 \leq i \leq r$ *y así para cada* $n \in \mathbb{N} \setminus \{0\}$, *se tiene*

$$x^n = nx = (nx_1, \ldots, nx_i, \ldots, nx_r) \neq (0, \ldots, 0),$$

ya que $nx_i \neq 0$.

5. *Si* G *es finito, entonces* $G = T(G)$. *Para ver esto, observemos que si* $n = o(G)$, *entonces* $x^n = 1$ *para todo* $x \in G$ *y de ahí* $x \in T(G)$.

6. *El recíproco del apartado anterior es falso. Por ejemplo, consideremos el grupo* $G = \mathbb{Q}/\mathbb{Z}$, *que no es finito; si* p *y* q *son números primos distintos, entonces*

$$\frac{1}{p} + \mathbb{Z} \neq \frac{1}{q} + \mathbb{Z}.$$

Sin embargo $T(G) = G$ *ya que dado* $x = \dfrac{m}{n} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, *resulta*

$$nx = m + \mathbb{Z} = 0 + \mathbb{Z} = \mathbb{Z}.$$

7. *Si* G *es abeliano y* K *es un subgrupo de* G, *entonces* $T(K) = K \cap T(G)$. *Esto es obvio, ya que*

$$T(K) = \{x \in K : o(x) \text{ es finito } \} = K \cap T(G).$$

En particular, si K *es libre de torsión,* $K \cap T(G) = \{1\}$ *y si* G *es libre de torsión también lo es* K, *ya que en ese caso tenemos que* $T(G) = \{1\}$. *Por tanto* $T(K) = K \cap \{1\} = \{1\}$.

Ejemplo 3.1.3 *Sea* $G = \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_r\mathbb{Z}) \times \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{(s)}$.

Entonces $T(G) = \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_r\mathbb{Z}) \times \overbrace{\{0\} \times \cdots \times \{0\}}^{(s)}$ *y en consecuencia*

$$T(G) \cong \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_r\mathbb{Z})$$

vía la aplicación

$$(x_1, \ldots, x_r, 0, \ldots, 0) \longmapsto (x_1, \ldots, x_r).$$

Para verlo, observemos que,

$$\mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_r\mathbb{Z}) \times \overbrace{\{0\} \times \cdots \times \{0\}}^{(s)} \subseteq T(G)$$

ya que si $(x_1, \ldots, x_r, 0 \ldots, 0) \in \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_r\mathbb{Z}) \times \overbrace{\{0\} \times \ldots \times \{0\}}^{(s)}$, *entonces* $m(x_1, \ldots, x_r, 0, \ldots 0) = (0, \ldots, 0)$, *siendo* $m = \operatorname{mcm}(m_1, \ldots, m_r)$.

Recíprocamente, ningún elemento

$$x = (u_1 + m_1\mathbb{Z}, \ldots, u_r + m_r\mathbb{Z}, a_1, \ldots, a_s)$$

con algún $a_i \neq 0$ *tiene orden finito, pues*

$$nx = (nu_1 + m_1\mathbb{Z}, \ldots, nu_r + m_r\mathbb{Z}, na_1, \ldots, na_s)$$

y $na_i \neq 0$ *para cada* $n \in \mathbb{Z} \setminus \{0\}$.

Ejemplo 3.1.4 *Sea* $G = \mathbb{Z}/(m_1\mathbb{Z}) \times \cdots \times \mathbb{Z}/(m_r\mathbb{Z}) \times \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{(s)}$.

Entonces $G/T(G) = \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{(s)}$. *Para verlo, denotemos*

$$T = T(G) \qquad y \qquad \mathbb{Z}^s = \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{(s)}.$$

Consideremos la siguiente aplicación:

$$\begin{array}{rcl} f : \mathbb{Z}^s & \longrightarrow & G/T \\ (x_1, \ldots, x_s) & \longmapsto & (0 + m_1\mathbb{Z}, \ldots, 0 + m_r\mathbb{Z}, x_1, \ldots, x_s) + T. \end{array}$$

Se verifica:

- *f es homomorfismo ya que*

$$f[(x_1,\ldots,x_s)+(y_1,\ldots,y_s)] = f(x_1+y_1,\ldots,x_s+y_s) =$$
$$= [(0+m_1\mathbb{Z},\ldots,0+m_r\mathbb{Z},x_1+y_1,\ldots,x_s+y_s)+T] =$$
$$= [(0+m_1\mathbb{Z},\ldots,0+m_r\mathbb{Z},x_1,\ldots,x_s)+T]+$$
$$+[(0+m_1\mathbb{Z},\ldots,0+m_r\mathbb{Z},y_1,\ldots,y_s)+T] =$$
$$f(x_1,\ldots,x_s)+f(y_1,\ldots,y_s).$$

- *f es inyectiva ya que para todo $(x_1,\ldots,x_s)\in\mathbb{Z}^s$ tal que $f(x_1,\ldots,x_s) = T$, se tiene Entonces*

$$(0+m_1\mathbb{Z},\ldots,0+m_r\mathbb{Z},x_1,\ldots,x_s)+T = T.$$

Por tanto,

$$(0+m_1\mathbb{Z},\ldots,0+m_r\mathbb{Z},x_1,\ldots,x_s)\in T.$$

Así, por el Ejemplo 3.1.3, tenemos que $x_1 = \cdots = x_s = 0$.

- *Veamos que f es sobreyectiva. Para ello sea*

$$u = (a_1+m_1\mathbb{Z},\ldots,a_r+m_r\mathbb{Z},x_1,\ldots,x_s)+T\in G/T.$$

Entonces, por el Ejemplo 3.1.3, sabemos que

$$x = (a_1+m_1\mathbb{Z},\ldots,a_r+m_r\mathbb{Z},0,\ldots,0)\in T.$$

Por tanto,

$$u = (a_1+m_1\mathbb{Z},\ldots,a_r+m_r\mathbb{Z},x_1,\ldots,x_s)+T =$$
$$= [(a_1+m_1\mathbb{Z},\ldots,a_r+m_r\mathbb{Z},x_1,\ldots,x_s)+T]-$$
$$-[(a_1+m_1\mathbb{Z},\ldots,a_r+m_r\mathbb{Z},0,\ldots,0)+T] =$$
$$= [(0+m_1\mathbb{Z},\ldots,0+m_r\mathbb{Z},x_1,\ldots,x_s)+T] = f(x_1,\ldots,x_s).$$

3.2. Independencia lineal, generadores y bases

Definición 3.2.1 *Sea G un grupo abeliano.*

1. *Un subconjunto $\{x_1,\ldots,x_r\}$ de G, decimos que es linealmente independiente si*

$$n_1x_1+\cdots+n_rx_r = 0 \Longrightarrow n_1 = \cdots = n_r = 0,$$

donde $n_i\in\mathbb{Z}$, $1\leq i\leq r$.

2. *Decimos que G es finitamente generado si existe un subconjunto $\{x_1, \ldots, x_r\}$ de G tal que, para todo elemento x de G existen $n_1, \ldots, n_r \in \mathbb{Z}$ con*

$$x = n_1 x_1 + \cdots + n_r x_r.$$

En este caso diremos que el conjunto $\{x_1, \ldots, x_r\}$ es un sistema generador del grupo G. De hecho es la definición vista en el Capítulo 1.

3. *Decimos que un subconjunto $\{x_1, \ldots, x_r\}$ de G, es una base si es un sistema generador y es linealmente independiente.*

Proposición 3.2.2 *Sea G un grupo abeliano y sean $x_1, \ldots, x_s$ elementos de G. La aplicación*

$$\begin{aligned} f : \mathbb{Z}^s &\longrightarrow G \\ (n_1, \ldots, n_s) &\longmapsto n_1 x_1 + \cdots + n_s x_s, \end{aligned}$$

es un homomorfismo de grupos. Además, los x_i son linealmente independientes, sistema generador o base si y sólo si f es respectivamente monomorfismo, epimorfismo o isomorfismo.

La demostración se deja como ejercicio al lector.

Definición 3.2.3 *Un grupo abeliano libre es un grupo abeliano que admite una base. El cardinal de la base se llama rango del grupo.*

Observación 3.2.4 *Si un grupo abeliano finitamente generado admite una base, ésta será finita; por tanto los grupos abelianos libres finitamente generados son exactamente los isomorfos a $\mathbb{Z}^s$ para algún s.*

Observaciones 3.2.5 1. *Un grupo abeliano finitamente generado no necesariamente tiene base, como puede verse en el caso de $\mathbb{Z}_n$. Se verifica que $\{\overline{1}\}$ es sistema generador, pero no es linealmente independiente.*

2. *Dados dos grupos G_1 y G_2 tales que $G_1 \subseteq G_2$ y $\operatorname{rang}(G_1) = \operatorname{rang}(G_2)$, no se tiene necesariamente que $G_1 = G_2$. Podemos considerar el caso $2\mathbb{Z} \subset \mathbb{Z}$.*

3. *Todo grupo abeliano finitamente generado es cociente de $\mathbb{Z}^s$ para cierto $s \in \mathbb{N}$. Basta considerar la aplicación*

$$\begin{aligned} \phi : \mathbb{Z}^s &\longrightarrow G \\ e_i &\longmapsto x_i \end{aligned}$$

de la Proposición 3.2.2, para $\{x_1, \ldots, x_n\} \subseteq G$ un sistema de generadores, donde e_i representa a una s-upla con todas las componentes cero excepto la que ocupa el lugar i-ésimo que es 1. Se verifica que ϕ es un epimorfismo, de donde por el Primer Teorema de Isomorfía, se tiene

$$G \cong \mathbb{Z}^s / \ker(\phi).$$

4. *Si elegimos bases, existe una biyección natural entre los conjuntos* $Hom_{\mathbb{Z}}(\mathbb{Z}^r, \mathbb{Z}^s)$ *y* $M_{s\times r}(\mathbb{Z})$. *Para ello consideramos una base de* $\mathbb{Z}^r$ *y una base de* $\mathbb{Z}^s$. *Sean éstas* $\{u_1, \ldots, u_r\}$ *y* $\{v_1, \ldots, v_s\}$ *respectivamente. Entonces se tendrá que*

$$f(u_j) = \sum_{i=1}^{s} a_{ij} v_j, \qquad 1 \leq j \leq r.$$

Análogamente al caso de espacios vectoriales, la aplicación f *queda expresada por la matriz* $A \in M_{s\times r}$, *dada por*

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22} & \ldots & a_{2r} \\ \vdots & \vdots & \ldots & \vdots \\ a_{s1} & a_{s2} & \ldots & a_{sr} \end{pmatrix}.$$

Recíprocamente dada una matriz $A \in M_{s\times r}$, *una vez fijadas las bases, se tiene un homomorfismo,* $f \in Hom_{\mathbb{Z}}(\mathbb{Z}^r, \mathbb{Z}^s)$.

Antes de señalar algunas observaciones recordamos algunas ideas sobre el rango y el determinante de una matriz.

Definición 3.2.6 *Dada una matriz* $A \in M_{n\times m}(\mathbb{Z})$, *llamamos rango de la matriz* A, *al número máximo de columnas linealmente independientes.*

Análogamente a como se ha definido el concepto de determinante de una matriz cuadrada con coeficientes sobre un cuerpo, puede definirse el concepto de determinante de una matriz con coeficientes enteros, verificándose en este caso las mismas propiedades. En concreto señalamos las siguientes:

- Dadas dos matrices $A, B \in M_n(\mathbb{Z})$, se tiene

$$\det(AB) = \det(A)\det(B).$$

- Una matriz $A \in M_n(\mathbb{Z})$ es invertible si y sólo si $\det(A)$ es invertible en $\mathbb{Z}$.

También es posible definir el rango de una matriz cuadrada mediante determinantes. Así, el rango de una matriz A coincide con el orden del mayor menor no nulo de dicha matriz; es decir, que una matriz A tiene de rango el número natural h cuando existe al menos un menor de orden h distinto de cero, y todos los menores de órdenes superiores a h, si los hay, son nulos.

Observación 3.2.7 *Sea* $A \in M_{s\times r}(\mathbb{Z})$, $f : \mathbb{Z}^r \longrightarrow \mathbb{Z}^s$. *Entonces, por la Proposición 3.2.2, se verifica:*

1. *f es un monomorfismo si y sólo si las columnas de la matriz A son elementos linealmente independientes. Esto es equivalente a afirmar que* $\operatorname{rang}(A) = r$.

2. *f es un epimorfismo si y sólo si las columnas de la matriz A es un sistema generador .*

3. *f es un isomorfismo si y sólo si las columnas de A forman una base. Esto es equivalente a decir que* $\operatorname{rang}(A)=o(A)$, *y esto es si y sólo si A es invertible, es decir* $\det(A) = \pm 1$.

Si las columnas de A forman un sistema generador, entonces $\operatorname{rang}(A) = s$. *El recíproco no es cierto. Por ejemplo la matriz* (2) *define un homomorfismo* $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *no sobreyectivo, pero* $\operatorname{rang}((2)) = 1$.

Corolario 3.2.8 *Una familia de s elementos de $\mathbb{Z}^s$ es base si la matriz cuyas columnas están constituidas por esta familia tiene rango s.*

3.3. Rango de un grupo abeliano finitamente generado

Definición 3.3.1 *Dado G un grupo abeliano finitamente generado, llamaremos rango de G, y se denota por* $\operatorname{rang}(G)$, *al número máximo de elementos linealmente independientes en G.*

Observación 3.3.2 *Si H es un subgrupo de G, entonces* $\operatorname{rang}(H) \leq \operatorname{rang}(G)$. *Si H es subgrupo normal de G, entonces* $\operatorname{rang}(G/H) \leq \operatorname{rang}(G)$.

Teorema 3.3.3 *Si G es un grupo abeliano finitamente generado entonces todo subgrupo suyo también es finitamente generado y de rango finito.*

DEMOSTRACIÓN. En primer lugar, probaremos por inducción sobre s que todo subgrupo de $\mathbb{Z}^s$ es finitamente generado y de rango finito.

Si $s = 1$, entonces el resultado es cierto, ya que todo subgrupo de $\mathbb{Z}$ es de la forma $m\mathbb{Z}$, con $m \in \mathbb{N}$.

Sea $s > 1$ y supongamos que todos los subgrupos de $\mathbb{Z}^{s-1}$ son finitamente generados. Sea un subgrupo N de $\mathbb{Z}^s$. Consideremos el homomorfismo de grupos

$$\begin{aligned} f : N &\longrightarrow \mathbb{Z} \\ (n_1, \ldots, n_s) &\longmapsto n_1. \end{aligned}$$

Por la Proposición 2.2.8(1), $f(N)$ es subgrupo de $\mathbb{Z}$. Asimismo, existe $m \in \mathbb{N}$ tal que $f(N) = m\mathbb{Z}$. En particular, $m \in f(N)$. Por tanto, existe $x = (n_1, \ldots, n_s) \in N$ tal que $f(x) = m$. Veamos que

$$N = \ker(f) + \langle x \rangle.$$

Siempre se verifica que $ker(f) + \langle x \rangle \subseteq N$. Para la otra inclusión, sea $y = (y_1, \ldots, y_s) \in N$. Entonces

$$y_1 = f(y) \in f(N) = m\mathbb{Z}.$$

Por tanto, existe $a \in \mathbb{Z}$ tal que $y_1 = ma$. Por otro lado, tenemos que $y - ax \in N$, ya que N es un subgrupo. También se verifica que

$$f(y - ax) = f(y) - af(x) = y_1 - ma = 0.$$

Por tanto, $y - ax \in \ker(f)$. Así $y \in \ker(f) + \langle x \rangle$.

Consideremos el siguiente homomorfismo de grupos:

$$\begin{array}{rcl} \phi : \ker(f) & \longrightarrow & \mathbb{Z}^{s-1} \\ (0, n_2, \ldots, n_s) & \longmapsto & (n_2, \ldots, n_s) \end{array}$$

Como ϕ es un monomorfismo, se tiene que $\ker(f)$ es isomorfo a un subgrupo de $\mathbb{Z}^{s-1}$. Aplicando la hipótesis de inducción, tendremos que $\ker(f)$ es finitamente generado y de rango finito. Por tanto N es un subgrupo finitamente generado, al ser suma de dos subgrupos finitamente generados. Como $\langle x \rangle$ es cíclico,

$$\operatorname{rang}(\ker(f)) \leq \operatorname{rang}(N) \leq \operatorname{rang}(\ker(f)) + 1.$$

Sea ahora un subgrupo H arbitrario de un grupo abeliano finitamente generado G. Al ser G un grupo finitamente generado, podemos establecer un epimorfismo $f : \mathbb{Z}^s \longrightarrow G$ para cierto $s \in \mathbb{N}$. Así tenemos el siguiente diagrama conmutativo de homomorfismos de grupos:

$$\begin{array}{ccc} \mathbb{Z}^s & \xrightarrow{f} & G \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i} \\ f^{-1}(H) & \xrightarrow{f} & H \end{array}$$

donde las flechas verticales son las inclusiones canónicas y las horizontales son epimorfismos. Por la Proposición 2.2.8(2), $f^{-1}(H)$ es un subgrupo de $\mathbb{Z}^s$. Por tanto $f^{-1}(H)$ es un subgrupo finitamente generado. Así H es un subgrupo finitamente generado. Como G es de rango finito, también lo es H.

■

Vamos a ver a continuación algunas propiedades básicas del rango.

Proposición 3.3.4 *1. El rango es invariante por isomorfismos.*

2. *Sean G_1, G_2 grupos abelianos y supongamos que G_2 es finitamente generado. Si $f : G_1 \longrightarrow G_2$ es un monomorfismo, entonces G_1 es finitamente generado y* $\operatorname{rang}(G_1) \leq \operatorname{rang}(G_2)$. *Si $f : G_2 \longrightarrow G_1$ es un epimorfismo, entonces G_1 es finitamente generado y* $\operatorname{rang}(G_1) \leq \operatorname{rang}(G_2)$.

3. *El rango de un grupo abeliano finito es cero.*

4. *El rango de $\mathbb{Z}^s$ es s.*

5. *Todas las bases de un grupo abeliano finitamente generado libre tienen la misma cardinalidad, que coincide con su rango.*

6. *Si G es un grupo abeliano finitamente generado y N es un subgrupo de G, entonces*
$$\operatorname{rang}(G/N) = \operatorname{rang}(G) - \operatorname{rang}(N).$$

7. *Si G_1 y G_2 son grupos abelianos finitamente generados, entonces*
$$\operatorname{rang}(G_1 \times G_2) = \operatorname{rang}(G_1) + \operatorname{rang}(G_2).$$

DEMOSTRACIÓN.

(1) Basta tener en cuenta que la imagen mediante un isomorfismo de elementos linealmente independientes son también linealmente independientes.

(2) Si $f : G_1 \longrightarrow G_2$ es un monomorfismo, entonces por el Primer Teorema de Isomorfía se tiene que $G_1 \cong f(G_1)$. Así, por (1), $\operatorname{rang}(G_1) = \operatorname{rang}(f(G_1))$. Por otra parte $f(G_1)$ es subgrupo de G_2, y por el Teorema 3.3.3 se tiene que $f(G_1)$ es finitamente generado. Como $\operatorname{rang}(f(G_1)) \leq \operatorname{rang}(G_2)$, se tiene el resultado.

Sea $\{x_1, \ldots, x_r\}$ un sistema generador de G_2. Si $f : G_2 \longrightarrow G_1$ es un epimorfismo entonces se verifica que $\{f(x_1), \ldots, f(x_r)\}$ es un sistema generador de G_1. Por tanto G_1 es también finitamente generado. Por el Primer Teorema de Isomorfía $G_1 \cong G_2/\ker(f)$, de donde $\operatorname{rang}(G_1) \leq \operatorname{rang}(G_2)$.

(3) Sea G un grupo abeliano finito. Supongamos que el rango no sea cero. Entonces existirá al menos $x \in G$ tal que x es linealmente independiente. Por tanto podemos definir un monomorfismo $f : \mathbb{Z} \longrightarrow G$ dado por $f(n) = nx$. Pero esto es contradictorio con el hecho de que G es un grupo finito.

(4) Observemos que $\mathbb{Z}^s \subset \mathbb{Q}^s$. Dado $\{e_1, \ldots, e_n\}$ un subconjunto de $\mathbb{Z}^s$, vamos a demostrar el siguiente resultado:

$\{e_1, \ldots, e_n\}$ son $\mathbb{Z}$-linealmente independientes $\iff$ $\{e_1, \ldots, e_n\}$ son linealmente independientes como elementos del $\mathbb{Q}$-espacio vectorial $\mathbb{Q}^s$.

$\Longleftarrow$: Trivial.
$\Longrightarrow$: Consideremos una combinación lineal

$$q_1 e_1 + \cdots + q_n e_n = 0$$

donde $q_i = \dfrac{a_i}{b_i}$ con $1 \leq i \leq n$. Definimos

$$b = b_1 \cdots b_n \qquad \text{y} \qquad \widehat{b_i} = b_1 \cdots b_{i-1} b_{i+1} \cdots b_n.$$

Entonces se tiene

$$0 = b\,(q_1 e_1 + \cdots + q_n e_n) = b q_1 e_1 + \cdots + b q_n e_n = a_1 \widehat{b_1} e_1 + \cdots + a_1 \widehat{b_1} e_n,$$

pero $\{e_1, \ldots, e_n\}$ es un conjunto de elementos $\mathbb{Z}$-linealmente independientes. Por tanto, se tiene que $a_i \widehat{b_i} = 0$ para $1 \leq i \leq n$, de donde $a_i = 0$ y en consecuencia $q_i = 0$ para $1 \leq i \leq n$.

Con la afirmación anterior, como $\mathbb{Q}^s$ es un $\mathbb{Q}$-espacio vectorial de dimensión s, se tiene el resultado.

(5) Sea G un grupo abeliano finitamente generado y libre. Sean B y B' dos bases de G tales que $\operatorname{rang}(B) = r$ y $\operatorname{rang}(B') = s$. Entonces se tienen isomorfismos

$$f : \mathbb{Z}^r \longrightarrow G, \qquad g : \mathbb{Z}^s \longrightarrow G.$$

En particular, tendremos que $g^{-1} \circ f : \mathbb{Z}^r \longrightarrow \mathbb{Z}^s$ es un isomorfismo. Entonces, por (1), se verifica que $\operatorname{rang}(\mathbb{Z}^r) = \operatorname{rang}(\mathbb{Z}^s)$. Pero por (4) se tiene que $\operatorname{rang}(\mathbb{Z}^r) = r$ y $\operatorname{rang}(\mathbb{Z}^s) = s$. Así $r = s$.

(6) Supongamos que $\operatorname{rang}(G/N) = s$ y $\operatorname{rang}(N) = r$. Vamos a probar que $\operatorname{rang}(G) = r + s$. Es sencillo comprobar que, si $y_1, \ldots, y_r \in N$ son elementos linealmente independientes y $x_1 + N, \ldots, x_s + N \in G/N$ son linealmente independientes entonces los elementos

$$x_1, \ldots, x_s, y_1, \ldots, y_r$$

son también linealmente independientes en G. Por tanto $\operatorname{rang}(G) \geq r+s$. Para probar que $\operatorname{rang}(G) = r + s$, probaremos que cualquier familia que

tenga $r+s+1$ elementos es linealmente dependiente.

Consideremos $r+s+1$ elementos cualesquiera de G y sea $\{x_1,\ldots,x_t\}$ una subfamilia maximal con la propiedad de que sus clases $x_1+N,\ldots,x_t+N \in G/N$ sea linealmente independientes. Claramente se tiene que $t \leq s$ ya que $\operatorname{rang}(G/N) = s$. Así tiene sentido considerar $r+1$ elementos distintos de los x_i. Veamos que los elementos

$$x_1,\ldots,x_t,y_1,\ldots,y_{r+1},$$

son linealmente dependientes.

Para cualquier y_i, los elementos

$$x_1+N, x_2+N,\ldots,x_t+N, y_i+N$$

son linealmente dependientes (por la maximalidad de t). Por tanto. se tienen las siguientes relaciones

$$\begin{array}{ccccccccc}
m_{11}x_1 & + & \cdots & + & m_{1t}x_t & + & n_1y_1 & = & z_1 \in N \\
m_{21}x_1 & + & \cdots & + & m_{2t}x_t & + & n_2y_2 & = & z_2 \in N \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
m_{(r+1)1}x_1 & + & \cdots & + & m_{(r+1)t}x_t & + & n_{(r+1)}y_{(r+1)} & = & z_{(r+1)} \in N,
\end{array}$$

donde $n_i \neq 0$ para todo $i = 1,\ldots,r+1$, (de nuevo por la maximalidad de t).

Por otra parte como $\operatorname{rang}(N) = r$, entonces los elementos $z_1,\ldots,z_{r+1} \in N$ son linealmente dependientes, es decir se tiene una relación del tipo

$$a_1z_1+\cdots+a_{r+1}z_{r+1} = 0,$$

para algún $a_i \neq 0$. Así tenemos que

$$\left(\sum_{j=1}^{r+1} a_jm_{j1}\right)x_1+\cdots+\left(\sum_{j=1}^{r+1} a_jm_{jt}\right)x_t+\sum_{j=1}^{r}(a_jn_j)y_j = 0$$

con algún $a_in_i \neq 0$. Así queda probado el resultado.

(7) Como se tienen los siguientes isomorfismos

$$\{0\}\times G_2 \cong G_2, \qquad (G_1\times G_2)/G_2 \cong G_1,$$

por (1) concluimos $\operatorname{rang}((G_1\times G_2)/G_2) = \operatorname{rang}(G_1)$ y por (7) concluimos $\operatorname{rang}(G_1\times G_2) - \operatorname{rang}(G_2) = \operatorname{rang}(G_1)$.

■

3.4. PAQ Reducción con coeficientes enteros

Definición 3.4.1 *Llamaremos operaciones elementales por columnas de una matriz $A \in M_{s\times r}(\mathbb{Z})$, a las siguientes transformaciones:*

1. *Permutar dos columnas.*
2. *Multiplicar una columna por -1.*
3. *Sumar a una columna un múltiplo entero de otra.*

Observación 3.4.2 *Aplicar una transformación elemental por columnas a una matriz $A \in M_{s\times r}(\mathbb{Z})$, equivale a multiplicar la matriz A por la derecha por una determinada matriz inversible de orden r. Es decir, multiplicar la matriz A por la derecha por las matrices:*

$$Q_1 = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & & 1 & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & 1 & & & 0 & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix},$$

$$Q_2 = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \quad Q_3 = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & \vdots & \ddots & & \\ & & \pm n & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

equivale, respectivamente, a intercambiar dos columnas, multiplicar una columna por -1 y sumar a una columna, otra multiplicada por $\pm n$. Si aplicamos a una matriz una cadena de transformaciones elementales y cada transformación equivale a multiplicar por $Q_1, Q_2, \cdots, Q_n$, el resultado final será la matriz producto: $AQ_1Q_2\cdots Q_n$. En la práctica para obtener la matriz de los cambios, aplicamos las transformaciones a la matriz

$$\begin{pmatrix} A \\ I_r \end{pmatrix}$$

donde I_r representa a la matriz identidad de orden r. Así, en cada momento del proceso, si multiplicamos a la derecha por la matriz Q (producto de las matrices elementales), tenemos que

$$\begin{pmatrix} A \\ I_r \end{pmatrix} Q = \begin{pmatrix} AQ \\ I_r Q \end{pmatrix} = \begin{pmatrix} AQ \\ Q \end{pmatrix}.$$

Por tanto tenemos una matriz dividida en dos submatrices, donde la submatriz de la parte superior es el resultado de aplicar las transformaciones y la submatriz inferior es la matriz Q, que relaciona el resultado obtenido con la matriz original.

Lema 3.4.3 *Sea* $\begin{pmatrix} a & b \\ & * \end{pmatrix} \in M_2(\mathbb{Z})$. *Entonces existe* $U \in GL_2(\mathbb{Z})$ *tal que*

$$\begin{pmatrix} a & b \\ & * \end{pmatrix} U = \begin{pmatrix} d & 0 \\ & * \end{pmatrix}$$

con $d = \text{mcd}(a, b)$.

DEMOSTRACIÓN. Por la Identidad de Bézout, existen $a_1, b_1 \in \mathbb{Z}$ tales que $d = aa_1 + bb_1$. Además, al ser $d = \text{mcd}(a, b)$, existen $a', b' \in \mathbb{Z}$ tales que $a = da'$ y $b = db'$. Así

$$d = aa_1 + bb_1 = da'a_1 + db'b_1 = d(a'a_1 + b'b_1).$$

Por tanto

$$1 = a'a_1 + b'b_1.$$

Sea $U = \begin{pmatrix} a_1 & -b' \\ b_1 & a' \end{pmatrix}$. Entonces $\det(U) = a_1a' + b_1b' = 1$, de donde $U \in GL_2(\mathbb{Z})$. Además

$$\begin{pmatrix} a & b \\ & * \end{pmatrix} \begin{pmatrix} a_1 & -b' \\ b_1 & a' \end{pmatrix} = \begin{pmatrix} aa_1 + bb_1 & -ab' + a'b \\ & * \end{pmatrix} = \begin{pmatrix} d & 0 \\ & * \end{pmatrix},$$

ya que

$$d = aa_1 + bb_1, \text{ y } -ab' + a'b = -da'b' + a'db' = 0.$$

■

Obviamente, esto también se puede hacer mediante operaciones elementales por columnas. Por el algoritmo de Euclides

$$\text{mcd}(a, b) = \text{mcd}(b, r) \text{ con } a = bq + r,\ r = 0 \quad \text{ó} \quad |r| < |b|,$$

$$\text{mcd}(b, r) = \text{mcd}(r, r_1) \text{ con } b = rq_1 + r_1,\ r_1 = 0 \quad \text{ó} \quad |r_1| < |r|.$$

Entonces

$$\begin{pmatrix} a & b \\ & * \end{pmatrix} \to \begin{pmatrix} r & b \\ & * \end{pmatrix} \to \begin{pmatrix} r & r_1 \\ & * \end{pmatrix} \to \cdots \to \begin{pmatrix} d & r_m \\ & * \end{pmatrix} \to \begin{pmatrix} d & 0 \\ & * \end{pmatrix}.$$

Proposición 3.4.4 *Mediante transformaciones elementales por columnas, toda matriz $A \in M_{s\times r}(\mathbb{Z})$ puede transformarse en una matriz escalonada de la forma*

$$\begin{pmatrix}
d_1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
d_2 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
* & \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\
* & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
* & d_3 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
* & * & \vdots & \cdots & \cdots & \cdots & \cdots & \vdots \\
* & * & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
* & * & \ddots & \cdots & \cdots & \cdots & \cdots & \vdots \\
* & * & * & d_t & 0 & \cdots & \cdots & 0 \\
* & * & * & * & \vdots & \cdots & \cdots & \vdots \\
* & * & * & * & 0 & \cdots & \cdots & 0
\end{pmatrix}$$

donde $di \in \mathbb{Z} \setminus \{0\}$ para todo i.

Demostración. Nos fijamos en la primera fila, digamos $(a_{i1}, \ldots, a_{ir})$, no nula de la matriz

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & & \vdots \\ a_{s1} & \cdots & a_{sr} \end{pmatrix},$$

y efectuamos el siguiente proceso:

(1) Aplicamos el procedimiento descrito en el Lema 3.4.3 a las submatrices 2×2 obtenidas fijando la primera fila no nula y la inmediata inferior, y dos columnas con coeficientes no nulos. Aplicado a lo sumo r veces, obtenemos una matriz equivalente donde aparezca d_1 en la primera posición de la primera fila y ceros en todos los otros lugares de la fila.

(2) A continuación repetimos este proceso con la primera fila no nula de la submatriz que queda al eliminar la primera fila no nula y la primera columna de la matriz. Aplicando repetidas veces el proceso, se concluye el resultado.

■

Observación 3.4.5 *Si multiplicamos la matriz $A \in M_{s\times r}(\mathbb{Z})$ por la derecha por una matriz arbitraria $Q \in M_{r\times t}(\mathbb{Z})$, las columnas del producto AQ son combinación lineal de las columnas de A. En particular si $Q \in GL_r(\mathbb{Z})$, las columnas de AQ generan el mismo subgrupo de $\mathbb{Z}^s$ que las columnas de A.*

Corolario 3.4.6 *Todo subgrupo de un grupo abeliano finitamente generado libre es libre.*

DEMOSTRACIÓN. Sea G un grupo abeliano finitamente generado y libre. Por la Observación 3.2.4, $G \cong \mathbb{Z}^s$ para algún s. Sea N un subgrupo de G. Entonces N es un subgrupo de $\mathbb{Z}^s$, y por el Teorema 3.3.3, N es grupo abeliano finitamente generado. Consideremos la matriz A cuyas columnas son un sistema generador para N. Por la Proposición 3.4.4, haciendo transformaciones elementales por columnas en la matriz A, podemos obtener una matriz escalonada. Por la Observación 3.4.5, las columnas de la matriz escalonada forman también un sistema generador de N. Como estas columnas son linealmente independientes, forman de hecho una base. Por lo tanto N es un grupo abeliano libre finitamente generado.

■

Podemos considerar también, de la misma forma que lo hemos hecho para las columnas, transformaciones elementales por filas. En este caso hacer transformaciones por filas equivale a multiplicar a la izquierda a la matriz dada por matrices elementales. De la misma forma que antes, si unimos a la matriz A la matriz identidad a la izquierda, y hacemos las transformaciones por filas a la matriz $(I|A)$, entonces en la posición de la matriz I aparece la matriz P, producto de todas las matrices elementales que han intervenido. Es decir:

$$(I|A) \longrightarrow P\,(I|A) \longrightarrow (P|PA)\,.$$

También podemos realizar transformaciones por filas y columnas de forma indiscriminada y sin preocuparnos del orden en el que hacemos las transformaciones. En la práctica, para obtener las matrices P y Q que recogen estas transformaciones, consideramos

$$\begin{pmatrix} I_s & A \\ 0 & I_r \end{pmatrix} \longrightarrow \begin{pmatrix} P & PAQ \\ 0 & Q \end{pmatrix}.$$

En virtud de todo ello, obtenemos el siguiente resultado, cuya demostración queda como ejercicio para el lector.

Proposición 3.4.7 *Dada una matriz $A \in M_{s\times r}(\mathbb{Z})$, existen $P \in GL_s(\mathbb{Z})$ y $Q \in GL_r(\mathbb{Z})$ tales que*

$$PAQ = \begin{pmatrix} d_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & d_t & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

donde $d_i \in \mathbb{Z} \setminus \{0\}$, para todo $i = 1, \cdots, t$.

Notación 3.4.8 *Dada una matriz $B \in M_{s\times r}(\mathbb{Z})$, denotemos por $\Delta_i(B)$ el máximo común divisor de todos sus menores de orden i.*

Lema 3.4.9 *Consideremos la matriz $A \in M_{s\times r}(\mathbb{Z})$. Sean $P \in GL_s(\mathbb{Z})$ y $Q \in GL_r(\mathbb{Z})$ las matrices cuya existencia asegura la Proposición 3.4.7. Entonces se tiene*

$$\Delta_i(A) = \Delta_i(AQ) = \Delta_i(PA), \qquad \text{para todo } i.$$

DEMOSTRACIÓN. Como P y Q son producto de matrices elementales, basta demostrar el resultado para matrices elementales P y Q.

Para cambios del tipo 1 ó 2, por filas o columnas, A, PA, AQ sólo cambia el orden de dos filas o columnas, de donde el resultado es obvio. En las del tipo 3 como el máximo común divisor no varía por combinaciones lineales, el resultado es claro.

■

Teorema 3.4.10 *Dada una matriz $A \in M_{s\times r}(\mathbb{Z})$, existen $P \in GL_s(\mathbb{Z})$ y $Q \in GL_r(\mathbb{Z})$ tales que*

$$PAQ = \begin{pmatrix} d_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & d_t & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

donde $d_i \in \mathbb{Z}^+$, $d_1|d_2|\cdots|d_t$. En estas circunstancias los d_i son únicos y se denominan factores invariantes de la matriz A. De hecho se verifica para cada i, $\Delta_i(A) = d_1 \cdots d_i$.

DEMOSTRACIÓN. Sea d_1 el máximo común divisor de todos los elementos de la matriz, es decir $d_1 = \text{mcd}(a_{ij})$, $A = (a_{ij})$. Por transformaciones elementales de filas y columnas podemos situar al número entero d_1 en la posición $(1,1)$ y hacer ceros todos los elementos de la primera fila y de la primera columna. La razón es que, por la Proposición 3.4.7,

$$A \longrightarrow \begin{pmatrix} \overline{d}_1 & 0 & \cdots & 0 & 0 \\ 0 & \overline{d}_2 & 0\cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & \overline{d}_t & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} \overline{d}_1 & \overline{d}_2 & \cdots & \overline{d}_t & 0 \\ 0 & \overline{d}_2 & 0\cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & \overline{d}_t & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow$$

$$\longrightarrow \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix},$$

donde $d_1 = \text{mcd}(\overline{d}_1, \ldots, \overline{d}_t) = \text{mcd}(a_{ij}) = \Delta_1(A)$.

Aplicamos el mismo razonamiento a la matriz A_1 y obtenemos

$$A_1 \longrightarrow \begin{pmatrix} d_2 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A_2 & \\ 0 & & & \end{pmatrix}$$

con $d_1 | d_2$ y como $d_1 d_2 = \Delta_2(A)$, ya que $d_1 d_2$ es un determinante de un menor 2×2, y como d_1, d_2, $d_1 d_2$ divide a todo menor 2×2, dividen a todo elemento de A_2. Aplicando nuevamente el argumento construimos una sucesión

$$d_1 | d_2 | \cdots | d_i,$$

con $d_1 d_2 \cdots d_i = \Delta_i(PAQ)$. Por el Lema 3.4.9 se tiene que $\Delta_i(PAQ) = \Delta_i(A)$ y de ahí el resultado.

■

3.5. Clasificación de los grupos abelianos finitamente generados

Teorema 3.5.1 (Teorema de Estructura) *Todo grupo abeliano finitamente generado es producto finito de grupos cíclicos.*

DEMOSTRACIÓN. Sea G un grupo abeliano finitamente generado. Consideremos $\{x_1, \ldots, x_s\}$ un sistema generador de G. Podemos establecer el siguiente epimorfismo

$$\begin{aligned} f : \mathbb{Z}^s &\longrightarrow G \\ (a_1, \ldots, a_s) &\longmapsto a_1x_1 + \cdots + a_sx_s. \end{aligned}$$

Por el Primer Teorema de Isomorfía, $\mathbb{Z}^s/\ker(f) \cong G$. Por otra parte, al ser $\ker(f)$ un subgrupo de $\mathbb{Z}^s$, se tiene que es libre finitamente generado por el Corolario 3.4.6. Así $\ker(f) \cong \mathbb{Z}^r$. Por tanto $\ker(f)$ tiene una base de r elementos. Consideremos la matriz $A \in M_{s\times r}(\mathbb{Z})$ cuyas columnas sean la base del $\ker(f)$ que hayamos escogido. Efectuamos sobre la matriz A la PAQ reducción, para obtener la forma

$$PAQ = \begin{pmatrix} d_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & d_t & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{i}$$

de la Proposición 3.4.7. Por la Observación 3.4.5, las columnas de AQ forman un un sistema generador de $\ker(f)$. Así

$$G \cong \mathbb{Z}^s/\ker(f) = \mathbb{Z}^s/A(\mathbb{Z}^r) = \mathbb{Z}^s/AQ(\mathbb{Z}^r).$$

Como $P \in GL_s(\mathbb{Z})$, P establece un isomorfismo de $\mathbb{Z}^s$ en $\mathbb{Z}^s$. Por tanto

$$\mathbb{Z}^s/AQ(\mathbb{Z}^r) \cong P(\mathbb{Z}^s)/PAQ(\mathbb{Z}^r) = \mathbb{Z}^s/PAQ(\mathbb{Z}^r),$$

y observemos que, por (i), $PAQ(\mathbb{Z}^r)$ es un grupo libre con base

$$\{(d_1, 0, \ldots, 0), (0, d_2, \ldots, 0), \ldots, (0, 0, \ldots, 0, d_t, 0, \ldots, 0)\}.$$

Como, al aplicar P a $\mathbb{Z}^s$ y a $AQ(\mathbb{Z}^r)$, estamos mirando ambos grupos respecto a la misma base de $\mathbb{Z}^s$, tenemos

$$\begin{aligned} \mathbb{Z}^s/PAQ(\mathbb{Z}^r) &\cong \mathbb{Z}^s/\left(d_1\mathbb{Z} \times \cdots \times d_t\mathbb{Z}\right) \times \{0\} \times \cdots \times \{0\} \cong \\ &\cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t \times \mathbb{Z} \times \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{(s-t)}. \end{aligned}$$

■

Corolario 3.5.2 *1. Todo grupo abeliano finito es isomorfo a un producto finito de grupos de la forma $\mathbb{Z}/n\mathbb{Z}$.*

2. *Un grupo abeliano finitamente generado tiene rango cero si y sólo si es finito.*

3. *Todo grupo abeliano finitamente generado es isomorfo a un producto de un grupo finito por un grupo abeliano libre.*

4. *Todo grupo abeliano finitamente generado es isomorfo al producto de un grupo de torsión por un grupo libre de torsión.*

5. *Un grupo abeliano finitamente generado libre de torsión es libre.*

Nuestro próximo objetivo es demostrar el Teorema de Clasificación de grupos abelianos finitamente generados. Para ello son necesarios algunos resultados previos que demostramos a continuación.

Lema 3.5.3 *Sean G_1 y G_2 dos grupos abelianos finitos. Se tiene que:*

$$G_1 \times \mathbb{Z}^r \cong G_2 \times \mathbb{Z}^s \Longleftrightarrow r = s \text{ y } G_1 \cong G_2.$$

DEMOSTRACIÓN. $\Longleftarrow$: Evidente.
$\Longrightarrow$: Por las propiedades (3) y (4) del rango vistas en la Proposición 3.3.4 se tiene que

$$r = \operatorname{rang}(\mathbb{Z}^r) = \operatorname{rang}(G_1 \times \mathbb{Z}^r) = \operatorname{rang}(G_2 \times \mathbb{Z}^s) = \operatorname{rang}(\mathbb{Z}^s) = s.$$

Por otro lado, observemos que:

- Las partes de torsión de dos grupos isomorfos son isomorfas. Vamos a verlo:
  Sea $f : G_1 \times \mathbb{Z}^s \longrightarrow G_2 \times \mathbb{Z}^s$. Si $x \in T(G_1)$ con $x \neq 1$, entonces $1 < o(f(x)) < \infty$. Por tanto $f(x) \in T(G_2)$, es decir $f(T(G_1)) \subseteq T(G_2)$. Como $f^{-1}(T(G_2)) \subset T(G_1)$, se tiene $f(T(G_1)) = T(G_2)$.

- Si G_1 es un grupo finito, entonces por la Observación 3.1.2(5), $T(G_1) = G_1$.

- $T(G_1 \times \mathbb{Z}^r) \cong G_1 \times \{0\} \cong G_1$ por el Ejemplo 3.1.3.

Por tanto

$$G_1 \cong G_1 \times \{0\} \cong T(G_1 \times \mathbb{Z}^r) \cong T(G_2 \times \mathbb{Z}^r) \cong G_2 \times \{0\} \cong G_2.$$

■

Lema 3.5.4 *Sea G un grupo abeliano finito tal que $o(G) = d$ y sea $p \in \mathbb{N}$ un número primo. Si p no divide a d entonces la aplicación*

$$\begin{aligned} \phi : G &\longrightarrow G \\ x &\longmapsto px \end{aligned}$$

es un isomorfismo.

DEMOSTRACIÓN.

- ϕ es un homomorfismo de forma natural.
- Veamos que ϕ es inyectiva. Si $x \in \ker(\phi)$ entonces se tiene que $px = 0$. Como p es un número primo que no divide a d, se tiene que $\text{mcd}(p, d) = 1$. Entonces, por la Identidad de Bézout, existen $a, b \in \mathbb{Z}$ tales que $1 = ap + bd$. Como $o(G) = d$, se tiene que $dx = 0$ para todo $x \in G$. Por tanto, para todo $x \in \ker(\phi)$ se tiene que

$$x = x(ap + bd) = apx + bdx = 0,$$

de donde $\ker(\phi) = \{0\}$. Así ϕ es un homomorfismo inyectivo, y al ser G finito se tiene que ϕ es un isomorfismo.

■

Lema 3.5.5 *Sean $0 \leq i < r$ números naturales y p un número primo. Consideremos el homomorfismo:*

$$\begin{aligned} \varphi_i : \mathbb{Z}/p^r\mathbb{Z} &\longrightarrow \mathbb{Z}/p^r\mathbb{Z} \\ x + p^r\mathbb{Z} &\longmapsto p^i x + p^r\mathbb{Z}. \end{aligned}$$

Entonces el cardinal de $\ker(\varphi_i)$ es p^i.

DEMOSTRACIÓN. Para todo elemento $x + p^r\mathbb{Z}$ se tiene un único representante $a \in \mathbb{Z}$ tal que $0 \leq a < p^r$. Este representante se puede escribir de forma única como

$$a = a_0 + a_1 p + \cdots + a_{r-1}p^{r-1}, \qquad 0 \leq a_i < p$$

(es decir, estamos escribiendo a en base p). Entonces

$$p^i a \equiv 0 \,(\text{mód } p^r\mathbb{Z}) \iff a_0 = a_1 = \cdots = a_{r-1-i} = 0.$$

Por tanto, los elementos de $\ker(\varphi_i)$ se obtienen por elección arbitraria de los i valores, $a_{r-i}, \ldots, a_{r-1}$, en el conjunto $\{0, \ldots, p-1\}$ de p valores. Luego $\text{card}\,(\ker(\varphi_i)) = p^i$.

■

Proposición 3.5.6 *Sean G_1 y G_2 dos grupos abelianos finitos y sea $p \in \mathbb{Z}$ un número primo tal que p no divide ni a $o(G_1)$ ni a $o(G_2)$. Si se tiene el siguiente isomorfismo de grupos:*

$$(\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_n}\mathbb{Z}) \times G_1 \cong (\mathbb{Z}/p^{b_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{b_m}\mathbb{Z}) \times G_2$$

con $1 \leq a_1 \leq \cdots \leq a_n$, $1 \leq b_1 \leq \cdots \leq b_m$. Entonces $n = m$ y $a_i = b_i$ para todo i.

DEMOSTRACIÓN. Si dos grupos son isomorfos, entonces tienen el mismo número de elementos anulados por p (concretamente, el producto del número de elementos anulados por p en cada factor). En G_1 y G_2 el único elemento anulado por p es el neutro. Por los Lemas 3.5.4 y 3.5.5, se tiene que el número de elementos anulados por p en cada factor distinto de G_1 y G_2 es p. Por tanto el número total de elementos anulados por p en el producto cartesiano es p^n y p^m respectivamente. Así $p^n = p^m$, de donde $n = m$.

Veamos a continuación que $a_i = b_i$ para todo i. Supongamos que sean distintos, entonces sea i_0 el menor subíndice tal que $a_{i_0} \neq b_{i_0}$ y podemos suponer sin pérdida de generalidad que $a_{i_0} < b_{i_0}$. En los subíndices $i < i_0$, tenemos el mismo número de elementos anulados por p en cada uno de los factores en los dos grupos. Por el Lema 3.5.5 en el grupo de la derecha hay p^{b_i} en el resto de los factores. En el grupo de la izquierda, también por el Lema 3.5.5, se tiene que el número de elementos es menor o igual que $p^{b_{i_0}}$ en el factor $\mathbb{Z}/p^{a_{i_0}}\mathbb{Z}$ y un número menor o igual que $p^{b_{i_0}}$ en el resto de los factores. Pero esto es contradictorio con el hecho de que debe de haber el mismo número de factores y de que los grupos son isomorfos.

■

Ahora ya estamos en condiciones de demostrar el Teorema de Clasificación de los grupos abelianos finitamente generados.

Teorema 3.5.7 (Teorema de Clasificación) *Todo grupo abeliano finitamente generado G es isomorfo exactamente a un grupo de la lista*

$$\mathbb{Z}^r \times \Pi_{i=1}^{t} \Pi_{j=1}^{j_i} \mathbb{Z}/p_{i_j}^{\alpha_j^i}\mathbb{Z},$$

con $p_1 < p_2 < \cdots < p_n$, y para cada $1 \leq i \leq t$, $\alpha_j^i \leq \alpha_{j+1}^i$, para todo $1 \leq j \leq j_i - 1$.

DEMOSTRACIÓN. Por el Teorema 3.5.1 se tiene que

$$G \cong \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{(r)} \times (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_t\mathbb{Z}).$$

Descomponiendo cada $d_i = \Pi_j p_{i_j}^{\alpha_j^i}$, y aplicando el Teorema Chino de los Restos tenemos

$$G \cong \mathbb{Z}^r \times \Pi_{i=1}^{t} \Pi_{j=1}^{j_i} \mathbb{Z}/p_{i_j}^{\alpha_j^i}\mathbb{Z},$$

con $p_1 < p_2 < \cdots < p_n$, y para cada $1 \leq i \leq t$, $\alpha_j^i \leq \alpha_{j+1}^i$, para todo $1 \leq j \leq j_i - 1$. Por tanto G es isomorfo a un grupo de la lista.

Veamos ahora la unicidad. Si tenemos que

$$G \cong \mathbb{Z}^s \times \Pi_{i=1}^{m} \Pi_{j=1}^{l_i} \mathbb{Z}/q_{i_j}^{\beta_j^i}\mathbb{Z},$$

entonces, por el Lema 3.5.3, $r = s$, y

$$\Pi_{i=1}^{t}\Pi_{j=1}^{j_i}\mathbb{Z}/p_{i_j}^{\alpha_j^i}\mathbb{Z} \cong \Pi_{i=1}^{m}\Pi_{j=1}^{l_i}\mathbb{Z}/q_{i_j}^{\beta_j^i}\mathbb{Z}.$$

Si existe p_i tal que $p_j \neq q_j$ para todo j, entonces por el Lema 3.5.4, p_i define un isomorfismo sobre $\Pi_{i=1}^{m}\Pi_{j=1}^{l_i}\mathbb{Z}/q_{i_j}^{\beta_j^i}\mathbb{Z}$, pero no sobre $\Pi_{i=1}^{t}\Pi_{j=1}^{l_i}\mathbb{Z}/p_{i_j}^{\alpha_j^i}\mathbb{Z}$, lo que es imposible. Por tanto cada p_i corresponde a un q_i, y por elección del orden, $p_i = q_i$, de donde $t = m$. Finalmente fijado p_i, por el Lema 3.5.5 concluimos que

$$\Pi_{i=1}^{t}\Pi_{j=1}^{j_i}\mathbb{Z}/p_{i_j}^{\alpha_j^i}\mathbb{Z} \cong \Pi_{i=1}^{m}\Pi_{j=1}^{l_i}\mathbb{Z}/q_{i_j}^{\beta_j^i}\mathbb{Z} \quad \text{con } j_i = l_i, \qquad \alpha_j^i = \beta_j^i,$$

de donde la expresión es única.

■

Proposición 3.5.8 *El recíproco del Teorema de Lagrange es cierto en los grupos abelianos finitos.*

DEMOSTRACIÓN. Es consecuencia directa del Teorema 3.5.1 y de la Proposición 1.5.17.

■

3.6. Ejercicios

1. Demostrad que el grupo $(\mathbb{Q}, +)$ es abeliano y que no admite un sistema finito de generadores.

2. Si G_1 y G_2 son dos grupos abelianos isomorfos, entonces también lo $G_1/T(G_1)$ y $G_2/T(G_2)$.

3. *a*) Sea G un grupo abeliano libre. Demostrad que G no tiene torsión.
   b) ¿Es libre el grupo aditivo de los números racionales?
   c) ¿Son libres todos los grupos abelianos sin torsión?

4. Sea G un grupo abeliano finitamente generado. Demostrad que las siguientes afirmaciones son equivalentes:
   a) G es libre.
   b) G no tiene torsión.
   c) Existe un entero positivo s tal que $G \cong \mathbb{Z}^s$.

5. ¿Es libre el grupo aditivo $\mathbb{R}$ de los números reales? ¿Lo es el grupo cociente $\mathbb{R}/\mathbb{Z}$?

6. Sea $G = \mathbb{R}/\mathbb{Q}$ el cociente del grupo aditivo $\mathbb{R}$ de los números reales respecto de su subgrupo $\mathbb{Q}$ de los números racionales.

   a) ¿Es $\mathbb{R}/\mathbb{Q}$ libre?

   b) Calculad $T(\mathbb{R}/\mathbb{Q})$.

   c) Estudiad si $\mathbb{R}/\mathbb{Q}$ es finitamente generado.

7. Probad que un grupo abeliano finito es no cíclico si y sólo si contiene un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ para algún primo p.

8. *a*) Demostrad que $H = \{(x, y, z, t) \in \mathbb{Z}^4 : x+y-z = 0\}$ es un subgrupo de $\mathbb{Z}^4$.

   b) Probad que H es libre y construid una base de H.

9. *a*) Escalonad por columnas la matriz

$$A = \begin{pmatrix} 6 & 0 & 6 & -12 \\ 2 & 64 & 16 & 24 \\ 3 & -64 & -10 & -36 \\ 11 & 0 & 12 & -24 \end{pmatrix},$$

   y calculad la matriz invertible de cambios.

   b) Diagonalizad la matriz resultante, calculando la matriz invertible de cambios por filas.

10. Dada la matriz A del ejercicio anterior:

    a) Encontrad una base del subgrupo de $\mathbb{Z}^4$ generado por sus columnas.

    b) Encontrad una base del núcleo de la aplicación $\mathbb{Z}^4 \to \mathbb{Z}^4$ definida por la matriz A.

11. Sea N el subgrupo generado por las columnas de la matriz A del ejercicio anterior. Demostrad que $\mathbb{Z}^4/N \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}$.

12. Decid si los siguientes subconjuntos de $\mathbb{Z} \times \mathbb{Z}$ constituyen bases:

    a) $\{(2,1), (3,1)\}$.

    b) $\{(2,1), (4,1)\}$.

Capítulo 4

Grupos de Permutaciones

Ésta es la segunda familia de grupos que estudiamos. Su importancia reside en que fueron los primeros grupos usados, introducidos por Abel, así como porque todo grupo es subgrupo de un grupo de permutaciones. Nosotros nos centraremos en los de orden finito, y los aplicaremos para obtener los grupos de simetría de polígonos regulares.

4.1. Teorema de Cayley. Consecuencias

Recordemos que, dado X un conjunto no vacío, denominaremos grupo de permutaciones de X, denotado $S(X)$, al grupo $Biy(X)$ de aplicaciones biyectivas de X en sí mismo. Si $\text{card}(X) = n$, identificamos X con el conjunto $E_n = \{1, \ldots, n\}$, y denotamos $S(X)$ como S_n.

Teorema 4.1.1 (Teorema de Cayley) *Todo grupo es isomorfo a un subgrupo de $S(X)$, para algún conjunto no vacío X apropiado.*

DEMOSTRACIÓN. Sea G un grupo, y tomemos $X = G$ (como conjunto). Definimos la aplicación

$$\begin{array}{rccccc} \phi: & G & \longrightarrow & S(X) & & \\ & g & \longmapsto & \phi_g : X & \longrightarrow & X \\ & & & x & \longmapsto & gx. \end{array}$$

Se verifica que:

- ϕ es homomorfismo de grupos, ya que si g_1, $g_2 \in G$, para todo $x \in X$ se tiene

$$\phi_{g_1 g_2}(x) = (g_1 g_2)(x) = g_1(g_2 x) = \phi_{g_1}(g_2 x) = \phi_{g_1}\left(\phi_{g_2}(x)\right) = \left(\phi_{g_1}\phi_{g_2}\right)(x),$$

de donde

$$\phi(g_1 g_2) = \phi_{g_1 g_2} = \phi_{g_1}\phi_{g_2} = \phi(g_1)\phi(g_2).$$

- Veamos que $\ker\phi = \{1\}$. Si $g \in \ker\phi$, entonces $\phi_g = Id_X$. Por tanto para todo $x \in X$ se tiene $\phi_g(x) = x$, es decir $gx = x$. En particular para $1 \in X$, se tiene $g1 = 1$, de donde $g = 1$.

Así por el Primer Teorema de Isomorfía, tenemos que $G \cong \phi(G)$, y al ser $\phi(G)$ un subgrupo de $S(X)$ obtenemos el resultado.

■

Si $\text{card}(G) = n$, entonces G es un subgrupo de S_n. Pero $\text{card}(S_n) = n!$, con lo que es relativamente grande. Intentemos ajustar el resultado.

Teorema 4.1.2 *Sean G un grupo y H subgrupo de G. Consideremos el conjunto $\Omega = \{xH : x \in G\}$. Entonces existe un morfismo de grupos $\phi : G \to S(\Omega)$ tal que $\ker(\phi)$ es el mayor subgrupo normal de G contenido en H.*

DEMOSTRACIÓN. Consideremos la aplicación

$$\begin{array}{rccccc} \phi: & G & \longrightarrow & S(\Omega) & & \\ & g & \longmapsto & \phi_g: & \Omega & \longrightarrow & \Omega \\ & & & & xH & \longmapsto & gxH. \end{array}$$

Análogamente a la demostración del Teorema 4.1.1, se tiene que ϕ es un morfismo.

- Por la Proposición 2.2.2 se tiene que $\ker(\phi)$ es un subgrupo normal de G.

- $\ker(\phi) \subseteq H$, ya que

$$\ker(\phi) = \{g \in G : gxH = xH, x \in G\}.$$

  Si $g \in \ker(\phi)$, en particular para $x = 1$, se tiene $gH = H$, de donde $g \in H$.

- Veamos que $\ker(\phi)$ es el mayor subgrupo con las propiedades anteriores. Sea N subgrupo normal de G tal que $N \subseteq H$. Entonces, para todo $n \in N$ y para todo $g \in G$ se tiene $g^{-1}ng \subseteq N \subset H$, es decir $g^{-1}ngH = H$. Así $ngH = gH$, de donde $n \in \ker(\phi)$.

■

Observación 4.1.3 *En el caso particular en que $H = \{1\}$, tenemos el Teorema de Cayley.*

Como consecuencia del Teorema 4.1.2 obtenemos

Corolario 4.1.4 *Sea G un grupo finito, y sea H un subgrupo de G tal que $o(G)$ no divide a $[G : H]!$. Entonces H contiene un subgrupo normal de G no trivial. En particular, G no puede ser simple.*

DEMOSTRACIÓN. Con la notación del Teorema 4.1.2, tenemos que $\text{card}(\Omega) = [G : H]$. Veamos que el homomorfismo $\phi : G \to S(\Omega)$ no es inyectivo. Si ϕ es monomorfismo entonces, por la Proposición 2.2.10, $o(\phi(G)) = o(G)$. Por hipótesis se tiene que $o(G)$ no divide a $[G : H]!$. Sin embargo $o(S(\Omega)) = [G : H]!$, contradiciendo el Teorema de Lagrange. Por tanto, $\ker(\phi)$ es un subgrupo normal de H no trivial.

■

Ejemplo 4.1.5 *1. Sea G un grupo tal que $o(G) = 36$. Supongamos que exista un subgrupo H de G tal que $o(H) = 9$ (veremos en el Capítulo 5 que así es). Entonces $[G : H] = 4$, y como 36 no divide a $4! = 24$, entonces existe N subgrupo normal de G siendo N subgrupo de H. Así G tiene un subgrupo normal de orden 3 ó 9.*

2. Sea G un grupo tal que $o(G) = 99$. Si existe un subgrupo H de G tal que $o(H) = 11$ (lo veremos en el Capítulo 5), entonces $[G : H] = 9$. Al verificarse que 99 no divide a $9!$, se tiene que existe N subgrupo normal de G, siendo N subgrupo de H. Como 11 es primo, concluimos que $N = H$. Por tanto, H es un subgrupo normal de G.

Ahora vamos a estudiar los grupos de permutaciones finitos.

4.2. Grupos de permutaciones finitos

Una biyección $\sigma \in S_n$ queda determinada, por la imagen de cada uno de los elementos $1, \cdots, n$. Para designarla utilizamos la notación

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Ejemplo 4.2.1 *Sea $n = 3$ y $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Entonces σ es la biyección en E_3 definida por*

$$\sigma(1) = 3, \qquad \sigma(2) = 1, \qquad \sigma(3) = 2.$$

Definición 4.2.2 *Sean n, k enteros positivos tales que $k \leq n$. Un elemento $\sigma \in S_n$ se llama ciclo de longitud k, si existe $\{a_1, \ldots, a_k\} \subseteq E_n$ tal que*

$$\begin{cases} \sigma(a_i) = a_{i+1} & 1 \leq i \leq k-1 \\ \sigma(a_k) = a_1 & \\ \sigma(a_j) = a_j & \forall\, j \in E_n \setminus \{a_1, \ldots, a_k\}. \end{cases}$$

Así, si σ es un ciclo de longitud k, denotado $\text{long}(\sigma) = k$, entonces σ es de la forma

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_k, a_j \dots \\ a_2 & a_3 & \dots & a_1, a_j \dots \end{pmatrix}.$$

y lo denotaremos por $\sigma = (a_1, \cdots, a_k)$.

Al conjunto $\{a_1, \dots, a_k\}$ lo llamaremos soporte del ciclo σ y lo denotaremos por $\text{supp}(\sigma)$.

Ejemplo 4.2.3 *El ciclo $\sigma = (1,4,5) \in S_6$ representa a la permutación*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix}.$$

Definición 4.2.4 *Los ciclos de longitud 2 se denominan trasposiciones.*

Observaciones 4.2.5 *Se tiene que:*

1. *La forma de escribir un ciclo de longitud k no es única. Así*

$$\sigma = (a_1, \dots, a_k) = (a_k, a_1, \dots, a_{k-1}) = \dots$$

Por tanto, las formas de escribir un mismo ciclo son las distintas maneras de elegir el primer elemento, que en este caso sería k. Luego un ciclo de longitud k puede escribirse de k formas distintas.

Ejemplo 4.2.6 *El ciclo $\sigma = (1,3,4)$ de S_4 puede escribirse como*

$$\sigma = (1,3,4) = (4,1,3) = (3,4,1),$$

y todos representan a la biyección

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

2. *Dos ciclos distintos pueden tener soportes iguales, como podemos ver en el siguiente ejemplo:*

Ejemplo 4.2.7 *Sean*

$$\sigma = (1,3,4) \qquad y \qquad \tau = (1,4,3).$$

Se verifica que

$$\text{supp}(\sigma) = \{1,3,4\} = \text{supp}(\tau),$$

pero sin embargo $\sigma \neq \tau$, ya que $\sigma(1) = 3$ y $\tau(1) = 4$.

3. *Dados los enteros positivos $a_1, \ldots, a_k$ puede resultar confuso hablar del ciclo $\sigma = (a_1, \ldots, a_k)$ si no se indica el grupo simétrico S_n al que pertenece σ. Por ejemplo:*

   Ejemplo 4.2.8 *Los ciclos*

   $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \in S_4 \qquad y \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \in S_5$$

   son distintos aunque ambos se escriban

   $$\sigma = (1, 3, 4) = \tau.$$

4. *Si $\sigma \in S_n$ es un ciclo de longitud 1, entonces σ es la identidad en E_n. Vamos a verlo: Sea σ es un ciclo de longitud 1. Entonces existe $a_1 \in E_n$ tal que*

   $$\sigma(j) = j \qquad \text{para cada} \qquad j \in E_n \setminus \{a_1\}.$$

   Pero como σ es una aplicación biyectiva, tendrá que verificarse $\sigma(a_1) = a_1$, y por tanto σ será la aplicación identidad.

Finalmente, podemos expresar cualquier ciclo como

$$(\sigma(a_1), \sigma^2(a_1), \ldots, \sigma^k(a_1)),$$

donde $a_1 \in \text{supp}(\sigma)$, $k \in \text{long}(\sigma)$.

Definición 4.2.9 *Dos ciclos σ, τ se denominan disjuntos si*

$$\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset.$$

En general, los ciclos no conmutan.

Ejemplo 4.2.10 *Sean $\sigma_1 = (1, 3, 5)$ y $\sigma_2 = (3, 5, 6)$ dos ciclos en S_6, entonces se tiene que:*

$$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix} \qquad y \qquad \sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 1 & 3 \end{pmatrix}.$$

Pero si los ciclos tienen la particularidad de que son disjuntos, entonces puede invertirse el orden de su composición sin alterar el resultado, tal como lo demuestra el siguiente resultado.

Proposición 4.2.11 *Sea $\sigma = (a_1, \ldots, a_k) \in S_n$ un ciclo de longitud $k \geq 2$. Entonces se verifica:*

1. *$\sigma^{-1} = (a_k, \ldots, a_1)$. En particular σ^{-1} es un ciclo de longitud k.*

2. *El orden de σ como elemento de S_n es k.*

3. *Si $\tau = (b_1, \ldots, b_l) \in S_n$ es un ciclo de longitud l, disjunto con τ, entonces $\sigma\tau = \tau\sigma$.*

DEMOSTRACIÓN.

(1) Si llamamos $\tau = (a_k, \ldots, a_1)$, vamos a probar que se verifica:

$$\tau\sigma(j) = \sigma\tau(j) = j \qquad \text{para cada} \qquad j \in E_n.$$

Se tiene que $\text{supp}(\sigma) = \text{supp}(\tau) = \{a_1, \ldots, a_k\}$. Consideremos los siguientes casos:

- Si $a_j \notin \{a_1, \ldots, a_k\}$. Entonces:

$$(\tau\sigma)(a_j) = \tau(\sigma(a_j)) = \tau(a_j) = a_j.$$

$$(\sigma\tau)(a_j) = \sigma(\tau(a_j)) = \sigma(a_j) = a_j.$$

- Si $a_j \in \{a_1, \ldots, a_k\}$. Entonces:

  (a) Para $1 < j < k$, se tiene

$$(\tau\sigma)(a_j) = \tau(\sigma(a_j)) = \tau(a_{j+1}) = a_j.$$

$$(\sigma\tau)(a_j) = \sigma(\tau(a_j)) = \sigma(a_{j-1}) = a_j.$$

  (b) Para a_k, se tiene

$$(\tau\sigma)(a_k) = \tau(\sigma(a_k)) = \tau(a_1) = a_k.$$

$$(\sigma\tau)(a_k) = \sigma(\tau(a_k)) = \sigma(a_{k-1}) = a_k.$$

  (c) Para a_1, se tiene

$$(\tau\sigma)(a_1) = \tau(\sigma(a_1)) = \tau(a_2) = a_1.$$

$$(\sigma\tau)(a_1) = \sigma(\tau(a_1)) = \sigma(a_k) = a_1.$$

Luego $\tau\sigma = \sigma\tau$ es la identidad y de ahí que $\tau = \sigma^{-1}$.

(2) Si $1 \leq i < k$, tendremos que

$$\sigma^i(a_1) = \sigma^{i-1}(\sigma(a_1)) = \sigma^{i-1}(a_2) = \sigma^{i-2}(\sigma(a_2)) =$$

$$\sigma^{i-2}(a_3) = \cdots = \sigma(a_i) = a_{i+1} \neq a_1,$$

luego σ^i no es la identidad, y así $o(\sigma) \geq k$. Por tanto es suficiente demostrar que $\sigma^k(j) = j$ para cada $j \in E_n$.

- Si $j \notin \text{supp}(\sigma)$, tendríamos $\sigma(j) = j$ y de ahí que $\sigma^k(j) = j$.
- Ahora, dado $1 \leq j \leq k$, se verifica

$$\sigma^{k-j+1}(a_j) = \sigma(a_k) = a_1.$$

Por lo tanto,

$$\sigma^k(a_j) = \sigma^{j-1}(a_1) = a_j.$$

(3) Supongamos que τ es la identidad. Entonces de forma obvia se verifica

$$\tau\sigma = \sigma\tau.$$

Supongamos $l \geq 2$ y $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$.
Notemos por $M = \text{supp}(\sigma) \bigcup \text{supp}(\tau)$, y consideremos los siguientes casos:

- Si $j \in E_n \setminus M$, se verifica que $\sigma(j) = j = \tau(j)$. Luego en este caso $(\sigma\tau)(j) = (\tau\sigma)(j)$.
- Si $j \in M$ entonces consideramos los siguientes casos:
  (a) Si $j \in \text{supp}(\sigma)$, $j \notin \text{supp}(\tau)$, entonces $\sigma(j) \in \text{supp}(\sigma)$ y así $\sigma(j) \notin \text{supp}(\tau)$, con lo que

$$(\sigma\tau)(j) = \sigma(j) = (\tau\sigma)(j).$$

  (b) Si $j \notin \text{supp}(\sigma)$, $j \in \text{supp}(\tau)$, el razonamiento es análogo, y se deja como ejercicio.

■

Los ciclos de S_n tienen interés porque constituyen un sistema generador de S_n, como vamos a demostrar a continuación.

Proposición 4.2.12 *Los ciclos constituyen un conjunto de generadores de S_n. Más concretamente, todo elemento de S_n se expresa como producto de ciclos disjuntos dos a dos de manera única (salvo el orden de los factores).*

DEMOSTRACIÓN. Sea $\sigma \in S_n$ y sea m_1 el menor entero positivo tal que $\sigma^{m_1}(1) = 1$. Tomemos

$$\sigma_1 = (1, \sigma(1), \ldots, \sigma^{m_1-1}(1)).$$

Ahora, sea i_1 el menor entero positivo en el conjunto $E_n \setminus \text{supp}(\sigma_1)$ y sea m_2 el menor entero positivo tal que $\sigma(i_1)^{m_2} = i_1$. Tomemos

$$\sigma_2 = (i_1, \sigma(i_1), \ldots, \sigma^{m_2-1}(i_1)).$$

Como E_n es finito, mediante la aplicación recurrente de este procedimiento, obtenemos un conjunto $\sigma_1, \sigma_2, \ldots, \sigma_l$ de ciclos en S_n.

Por construcción, los ciclos $\sigma_1, \sigma_2, \ldots, \sigma_l$ son disjuntos, ya que $\text{supp}(\sigma_r) \subseteq E_n \backslash \bigcup_{i=1}^{r-1} \text{supp}(\sigma_i)$, $1 < r \leq l$. Asimismo, por construcción, $\sigma|_{\text{supp}(\sigma_i)} = \sigma_i|_{\text{supp}(\sigma_i)}$ para todo $i \in \{1, \ldots, r\}$. Por tanto,

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_l.$$

La unicidad se deduce del hecho que los ciclos son disjuntos.

■

Ejemplo 4.2.13 *En S_7 se verifica que*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 1 & 2 & 4 \end{pmatrix} = (1,3,5)(2,6)(4,7).$$

Corolario 4.2.14 *Sea σ una permutación de S_n y $\sigma = \sigma_1 \sigma_2 \cdots \sigma_l$ una descomposición de σ en ciclos disjuntos. Entonces*

$$o(\sigma) = \text{mcm}\{o(\sigma_i) : 1 \leq i \leq l\}.$$

DEMOSTRACIÓN. Sean $m = o(\sigma)$, $m_i = o(\sigma_i)$, $1 \leq i \leq l$ y $s = \text{mcm}(m_1, \ldots, m_l)$. Como los ciclos σ_i son disjuntos, conmutan. Por tanto

$$\sigma^s = \sigma_1^s \sigma_2^s \cdots \sigma_l^s.$$

Por otro lado para cada i, $1 \leq i \leq l$, existe p_j un entero positivo tal que $s = m_j p_j$.

Así

$$\sigma^s = \sigma_1^{m_1 p_1} \sigma_2^{m_2 p_2} \cdots \sigma_l^{m_l p_l} = (\sigma_1^{m_1})^{p_1} (\sigma_2^{m_2})^{p_2} \cdots (\sigma_l^{m_l})^{p_l} = Id_{S_n}.$$

Por tanto, $m \leq s$. Si demostramos que $\sigma^k \neq Id_{S_n}$ para todo $1 \leq k \leq s-1$, tendremos que $m = s$.

Para demostrar esto, observemos que si $k < s$, como $s = \text{mcm}(m_1, \ldots, m_l)$, existe $j \in \{1, \ldots, l\}$ tal que k no es múltiplo de m_j. Por tanto, si consideramos el ciclo

$$\sigma_j = (i_{j-1}, \sigma_j(i_{j-1}), \ldots, \sigma_j^{m_j - 1}(i_{j-1})),$$

se tiene que

$$\sigma^k(i_{j-1}) = (\sigma_j)^k(i_{j-1}) \neq i_{j-1},$$

de donde $\sigma^k \neq Id$.

■

Ejemplo 4.2.15 *La permutación*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 6 & 5 \end{pmatrix} = (5,6)(1,3,4,2)$$

tiene orden $\text{mcm}(2,4) = 4$.

Ejemplo 4.2.16 *Para calcular el orden de* $\beta = (3,4,5)(1,5,2,4) \in S_5$ *realizamos su descomposición en ciclos disjuntos. Ésta es*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1,3,4)(2,5).$$

Por tanto, su orden es 6.

Proposición 4.2.17 *Todo ciclo se descompone en un producto de trasposiciones.*

DEMOSTRACIÓN. Sea $\sigma = (a_1, \ldots, a_k) \in S_n$. Entonces, por inducción sobre k, se demuestra que

$$(a_1, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2).$$

■

Corolario 4.2.18 *Las trasposiciones forman un sistema de generadores de* S_n.

Observación 4.2.19 *La descomposición de una permutación en trasposiciones no es única, como puede verse en el siguiente ejemplo en* S_6,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = (1,5)(2,6)(2,4) = (1,5)(6,4)(6,2) = (1,5)(4,6)(2,6).$$

Proposición 4.2.20 *Se tiene que*

1. *Las trasposiciones* $(1,2),(1,3),\ldots,(1,n)$ *generan* S_n.
2. *Las trasposiciones* $(1,2),(2,3),\ldots,(n-1,n)$ *generan* S_n.
3. *La trasposición* $(1,2)$ *y el ciclo* $(1,2,3,\ldots,n-1,n)$ *generan* S_n.

DEMOSTRACIÓN.

(1) Observemos que, para todo $a, b \in E_n$, se tiene

$$(a,b) = (1,a)(1,b)(1,a).$$

Por tanto, por la Proposición 4.2.17, se concluye el resultado.

(2) Mediante un argumento de inducción sobre k, se prueba que

$$(1,k) = (k-1,k)\cdots(3,4)(2,3)(1,2)(2,3)(3,4)\cdots(k-1,k),$$

de donde, por el apartado (1), concluimos el resultado.

(3) Mediante un argumento de inducción sobre k, se prueba que

$$(k,k+1) = (1,2,\ldots,n)^{k-1}(1,2)(1,2,\ldots,n)^{1-k},$$

de donde, por el apartado (2), concluimos el resultado.

■

Observación 4.2.21 *El conjunto* $\{(1,2),(1,2,3,\ldots,n-1,n)\}$ *es un sistema generador minimal de* S_n. *Esto es obvio para* $n=2$, *pues en tal caso* $(1,2) = (1,2,3,\ldots,n-1,n)$. *Si* $n \geq 3$, S_n *no es abeliano, y en particular no es cíclico, luego no está generado por un sólo elemento. Por tanto un sistema de generadores debe tener al menos dos elementos.*

Definición 4.2.22 *Dada* $\sigma \in S_n$, *donde*

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$$

y dados i,j *con* $1 \leq i < j \leq n$, *diremos que* $\sigma(i)$ *y* $\sigma(j)$ *están en inversión si* $\sigma(i) > \sigma(j)$.

Definición 4.2.23 *Dado* $\sigma \in S_n$, *definimos signo (o índice) de* σ, *denotado* $(-1)^\sigma$, *al número*

$$(-1)^\sigma = \begin{cases} 1 & \text{si el número de inversiones es par} \\ -1 & \text{si el número de inversiones es impar} \end{cases}$$

Proposición 4.2.24 *Sean* $\sigma \in S_n$ *e* $i,j \in E_n$ *con* $i \neq j$. *Denotemos por* $\overline{\sigma} = (i,j)\sigma$. *Entonces se verifica:*

$$(-1)^{\overline{\sigma}} = -(-1)^\sigma.$$

DEMOSTRACIÓN. Consideremos los siguientes casos:

i) Supongamos que $j = i+1$, y sean $k,l \in E_n$ tales que $\sigma(k) = i, \sigma(l) = j$. Como $\overline{\sigma} = (i,j)\sigma$, se tiene que $\overline{\sigma}|_{E_n\setminus\{k,l\}} = \sigma|_{E_n\setminus\{k,l\}}$. Como además i y j son contiguos, la variación de inversión entre $\overline{\sigma}$ y σ sólo afecta a estos dos elementos: si estaban en inversión en σ, dejan de estarlo en $\overline{\sigma}$, y al revés. Así, la permutación $(i,j)\sigma$ aumenta o disminuye en uno el número de inversiones.

ii) Si $j = i + p$ con $p > 1$, entonces (i, j) es la composición de p transposiciones (llevar i a j) más $p - 1$ transposiciones (llevar j desde la posición $j - 1$ a i). Por tanto (i, j) es composición de $2p - 1$ transposiciones contiguas, y por aplicación reiterada de (i), cambia la paridad.

■

Corolario 4.2.25 *Se verifica que:*

1. *Dado $\sigma \in S_n$, si $\sigma = \tau_1 \cdots \tau_r$, siendo $\{\tau_1, \ldots, \tau_r\}$ transposiciones, entonces*
$$(-1)^\sigma = (-1)^r.$$
2. *Si $\sigma_1, \sigma_2 \in S_n$, entonces $(-1)^{\sigma_1\sigma_2} = (-1)^{\sigma_1}(-1)^{\sigma_2}$.*

DEMOSTRACIÓN.

1. Se demuestra por inducción sobre r.
   - Para $r = 1$ es obvia, ya que en ese caso $\sigma = \tau_1$ y se verifica el resultado teniendo en cuenta la demostración del resultado anterior.
   - Supongamos cierto para $\sigma = \tau_1 \cdots \tau_{r-1}$, con $r > 1$, y lo demostramos para r. Sea $\sigma = \tau_1 \cdots \tau_r$. Notemos por $\tau = \tau_2 \cdots \tau_r$ y $\overline{\tau} = \tau_1\tau$. Se tiene que $\sigma = \overline{\tau}$. Por la Proposición 4.2.24, y aplicando la hipótesis de inducción, se tiene que:
   $$(-1)^\sigma = (-1)^{\overline{\tau}} = -(-1)^\tau = (-1)(-1)^{r-1} = (-1)^r.$$
2. Sean
   $$\sigma_1 = \tau_1 \cdots \tau_r \qquad \text{y} \qquad \sigma_2 = \tau_{r+1} \cdots \tau_s.$$
   Entonces, por el apartado anterior,
   $$(-1)^{\sigma_1\sigma_2} = (-1)^{r+s} = (-1)^r(-1)^s = (-1)^{\sigma_1}(-1)^{\sigma_2}.$$

■

Observamos que, como consecuencia del Corolario 4.2.25 se tiene el Teorema de Sylvester.

Teorema 4.2.26 (Teorema de Sylvester) *Sean*
$$\sigma = \alpha_1 \cdots \alpha_r, \qquad \sigma = \tau_1 \cdots \tau_r$$
dos descomposiciones de σ en producto de trasposiciones. Entonces
$$(-1)^r = (-1)^s.$$

Podemos clasificar las permutaciones según sea su índice y así tenemos

Definición 4.2.27 *Dada $\sigma \in S_n$, diremos que σ es par si $(-1)^\sigma = 1$. En caso contrario diremos que σ es impar.*

Como el signo de una permutación es multiplicativo, y $(\{1,-1\},\cdot)$ es un grupo multiplicativo, podemos establecer un epimorfismo de grupos dado por

$$\begin{array}{rccc} \varepsilon: & S_n & \to & (\{1,-1\},\cdot) \\ & \sigma & \to & (-1)^\sigma, \end{array}$$

donde $\ker(\varepsilon) = \{\sigma \in S_n : \sigma \text{ es par }\}$.

Observemos que, para todo $\sigma \in S_n$, $\epsilon(\sigma) = (-1)^\sigma$, es decir, $\epsilon(\sigma)$ representa el índice de la permutación σ.

Así, el conjunto de las permutaciones pares de S_n es un subgrupo normal de índice 2, llamado grupo alternado n-ésimo, denotado A_n. Se verifica que $o(A_n) = \dfrac{n!}{2}$.

Corolario 4.2.28 *Un ciclo σ de S_n pertenece a A_n si y sólo si tiene longitud impar.*

DEMOSTRACIÓN. Sea $\sigma = (a_1, \ldots, a_k) \in S_n$. Por la Proposición 4.2.17, existen trasposiciones $\tau_1, \ldots, \tau_{k-1}$ tales que

$$\sigma = \tau_1 \cdots \tau_{k-1}.$$

Por el Corolario 4.2.25 se tiene que

$$(-1)^\sigma = (-1)^{k-1}.$$

Así $\sigma \in A_n$ si y sólo si $k-1$ es par, esto es, si y sólo si k es impar.

■

4.3. Simplicidad de A_n. Teorema de Abel

El objetivo de esta sección es probar que para $n \neq 4$, A_n es un grupo simple. Al margen de su aplicación en el Capítulo 6, el interés del resultado reside en ser la clave del trabajo de Abel sobre resolubilidad por radicales de ecuaciones polinomiales.

Observemos que si $n = 2$, entonces $A_2 = \{1\}$. Por tanto podemos descartar este caso para cualquier cálculo.

Proposición 4.3.1 *Si $n \geq 3$, entonces*

1. *Cada ciclo $\sigma \in S_n$ de longitud 3 pertenece a A_n.*
2. *El ciclo $\beta = (1,2,3)$ genera A_3.*
3. *Si $n \geq 4$, e $i,j,u,v \in E_n$ son distintos, se tiene*

$$(i,u,v) = (i,j,v)(i,j,u)(i,j,u).$$

4. *Fijados $i,j \in E_n$ con $i \neq j$, denotamos*

$$\beta_k = (i,j,k), \quad \text{para cada} \quad k \in E_n \setminus \{i,j\}.$$

Entonces el conjunto de ciclos $C = \{\beta_k : k \in E_n \setminus \{i,j\}\}$ es un sistema de generadores de A_n.

DEMOSTRACIÓN.

(1) Obvio por el Corolario 4.2.28.

(2) Por el apartado (1), se tiene que $\langle\beta\rangle \subseteq A_3$. Por otro lado se verifica que

$$\beta^2 = (1,3,2), \qquad \beta^3 = Id,$$

es decir $o(\beta) = 3$. Pero

$$o(A_3) = \frac{3!}{2} = 3 = o(\beta),$$

de donde $\langle\beta\rangle = A_3$. Por Teorema 2.4.3, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$.

Así para $n = 3$ se tiene que $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ y de ahí que A_3 sea un grupo simple.

(3) Si notamos

$$\sigma = (i,u,v), \qquad \tau = (i,j,v), \qquad \beta = (i,j,u),$$

tenemos que probar $\sigma = \tau\beta^2$. Se tiene que:

- Si $x \in E_n \setminus \{i,j,u,v\}$, entonces

$$\sigma(x) = x = \tau\beta^2(x),$$

ya que $x \in E_n \setminus (\text{supp}(\sigma) \cup \text{supp}(\tau) \cup \text{supp}(\beta))$.

- $\tau\beta^2(i) = \tau(u) = u = \sigma(i)$.
- $\tau\beta^2(j) = \tau(i) = j = \sigma(j)$.

- $\tau\beta^2(u) = \tau(j) = v = \sigma(u)$.
- $\tau\beta^2(v) = \tau(v) = i = \sigma(v)$.

(4) Para $n = 3$, es el apartado (2). Supongamos $n \geq 4$ y sea $\sigma \in A_n \subset S_n$. Por el apartado (1) de la Proposición 4.2.20, se tiene que

$$\sigma = \tau_1' \cdots \tau_l'$$

con $\tau_s' = (1, h_s)$, $1 \leq s \leq l$, $h_s \in E_n \setminus \{1\}$. Fijado $i \in E_n$ arbitrario, el argumento de la Proposición 4.2.20(1) prueba que $(1, h_s) = (i, 1)(i, h_s)(i, 1)$. Por tanto, sin pérdida de generalidad podemos asumir que

$$\sigma = \tau_1 \cdots \tau_l$$

con $\tau_s = (i, h_s)$, $1 \leq s \leq l$, $h_s \in E_n \setminus \{i\}$.

Podemos suponer $h_s \neq h_{s+1}$, pues en caso contrario $\tau_s\tau_{s+1} = Id$, y podemos suprimirlas de la expresión. Como $\sigma \in A_n$, tenemos

$1 = \varepsilon(\sigma) = (-1)^l$, de donde $l = 2r$ para cierto $r \in \mathbb{N}$.

Así,

$$\sigma = (\tau_1\tau_2)\ldots(\tau_{2r-1}\tau_{2r}),$$

donde

$$\tau_{2t-1}\tau_{2t} = (i, h_{2t-1})(i, h_{2t}) =$$

$$= (h_{2t-1}, i)(i, h_{2t}) = (h_{2t-1}, i, h_{2t}) = (i, h_{2t}, h_{2t-1}).$$

Fijamos ahora $j \neq i$, y distinguimos:

(i) Si $h_{2t} \neq j \neq h_{2t-1}$, entonces $\tau_{2t-1}\tau_{2t} = \beta_{h2t-1}\beta_{h2t}^2$ por el apartado (3)

(ii) Si $j = h_{2t}$, entonces $\tau_{2t-1}\tau_{2t} = (i, j, h_{2t+1}) = \beta_{h_{2t-1}}$.

(iii) Si $j = h_{2t-1}$, entonces $\tau_{2t-1}\tau_{2t} = (i, h_{2t}, j) = \beta_{h_{2t}}^2$.

■

Lema 4.3.2 *Sea $n \geq 3$, y sea N un subgrupo normal de A_n que contiene un ciclo de longitud 3. Entonces $N = A_n$.*

DEMOSTRACIÓN. Si $n = 3$ el resultado es obvio, ya que $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, de donde $N = \{Id\}$ ó $N = \mathbb{Z}/3\mathbb{Z}$. Pero $\{Id\}$ no es ciclo de longitud 3.

Supongamos $n \geq 4$. Sea $\sigma = (j, i, a)$ el ciclo de longitud 3 en N cuya existencia asegura el enunciado. Utilizando la Proposición 4.3.1(4), es suficiente

probar que para cada $k \in E_n \setminus \{i,j\}$, $\beta_k = (i,j,k) \in N$, pues en tal caso, con la notación de la Proposición 4.3.1, se tiene $C \subseteq N$, de donde

$$A_n = \langle C \rangle \subseteq N \subseteq A_n.$$

Tenemos $\beta_a = (i,j,a) = \sigma^2$. Como $\sigma \in N$ también $\beta_a \in N$. Así, basta ver que $\beta_k \in N$ para cada $k \in E_n \setminus \{i,j,a\}$.

Ahora, como los elementos i,j,k,a, son distintos, tenemos $\tau_k = (i,j)(a,k) \in A_n$, ya que $\varepsilon(\tau_k) = 1$. Utilizando los apartados (1) y (3) de la Proposición 4.2.11, tenemos

$$\tau_k^{-1} = (a,k)^{-1}(i,j)^{-1} = (k,a)(j,i) = (j,i)(k,a) = (i,j)(a,k) = \tau_k.$$

Como $\tau_k \in A_n$ y N es un subgrupo normal de A_n, se tiene

$$\tau_k \sigma \tau_k \in N.$$

Por tanto, el lema quedará probado si comprobamos la igualdad

$$\tau_k \sigma \tau_k = \beta_k.$$

Es claro que para $x \in E_n \setminus \{i,j,k,a\}$ se cumple

$$\tau_k \sigma \tau_k(x) = x = \beta_k(x).$$

Además

- $\tau_k \sigma \tau_k(a) = \tau_k \sigma(k) = \tau_k(k) = a = \beta_k(a)$.
- $\tau_k \sigma \tau_k(k) = \tau_k \sigma(a) = \tau_k(j) = i = \beta_k(k)$.
- $\tau_k \sigma \tau_k(i) = \tau_k \sigma(j) = \tau_k(i) = j = \beta_k(i)$.
- $\tau_k \sigma \tau_k(j) = \tau_k \sigma(i) = \tau_k(a) = k = \beta_k(j)$.

■

Definición 4.3.3 *Sea n un entero positivo y $\sigma \in S_n$. Llamaremos parte fija de σ al conjunto*

$$F(\sigma) = \{x \in E_n : \sigma(x) = x\}.$$

Evidentemente, el único elemento de S_n cuya parte fija es E_n es la identidad. Denotaremos por $f(\sigma)$ al número de elementos de $F(\sigma)$. La prueba de la simplicidad de A_n para $n \geq 5$ se apoya en el estudio de la función

$$\begin{array}{rccc} f : & S_n & \longrightarrow & \mathbb{N} \\ & \sigma & \longmapsto & f(\sigma). \end{array}$$

Proposición 4.3.4 *Sea $n \geq 5$, y sea $\sigma = \tau_1 \cdots \tau_r \in S_n$, donde $\tau_1, \ldots, \tau_r$ son ciclos disjuntos dos a dos. Supongamos que $\tau_1 = (a_1, \ldots, a_k)$ con $k \geq 3$. Llamemos $\beta = (a_1, a_2, a_3)$. Entonces el elemento $\alpha = \sigma\beta^{-1}\sigma^{-1}\beta$ cumple $F(\sigma) \subsetneq F(\alpha)$, y en particular $f(\sigma) < f(\alpha)$. Además, si $k > 3$, α no es la identidad.*

DEMOSTRACIÓN. Como los ciclos son disjuntos dos a dos, se tiene

$$\begin{aligned} &\sigma(a_i) = \tau_1(a_i) = a_{i+1} \qquad \text{si} \quad 1 \leq i \leq k-1 \\ &\sigma(a_k) = \tau_1(a_k) = a_1 \neq a_k. \end{aligned}$$

Por tanto $F(\sigma) \subseteq E_n \setminus \operatorname{supp}(\tau_1)$.
Si $x \in F(\sigma)$, como $x \notin \{a_1, a_2, a_3\}$, se tiene

$$\beta(x) = x = \beta^{-1}(x), \qquad \sigma(x) = x = \sigma^{-1}(x),$$

de donde $\alpha(x) = x$. En consecuencia $F(\sigma) \subseteq F(\alpha)$.

Para demostrar que la inclusión es estricta, es suficiente comprobar que $a_2 \in F(\alpha)$. Como $k \geq 3$, tenemos

$$\beta(a_2) = a_3, \qquad \sigma^{-1}(a_3) = \tau_1^{-1}(a_3) = a_2,$$

y así

$$\alpha(a_2) = \sigma\beta^{-1}(a_2) = \sigma(a_1) = \tau_1(a_1) = a_2.$$

Por tanto $F(\sigma) \neq F(\alpha)$. Sólo falta ver que, cuando $k > 3$, α no es la identidad. Pero

$$\alpha(a_3) = \sigma\beta^{-1}\sigma^{-1}(a_1) = \sigma\beta^{-1}(a_k) = \sigma(a_k) = a_1 \neq a_3,$$

donde la tercera igualdad es porque, al ser $k > 3$, a_k no pertenece a

$$\operatorname{supp}(\beta^{-1}) = \operatorname{supp}(\beta) = \{a_1, a_2, a_3\}.$$

■

Proposición 4.3.5 *Sea $n \geq 5$, y sea $\sigma = \tau_1 \cdots \tau_r \in S_n$, donde $\tau_1, \ldots, \tau_r$ son ciclos disjuntos dos a dos (distintos de la identidad). Supongamos que $r \neq 1$ y que $\tau_1 = (a_1, a_2, a_3)$. Sea $a_4 \in \operatorname{supp}(\tau_2)$ y $\beta = (a_1, a_2, a_4)$. Entonces el elemento $\alpha = \beta\sigma\beta^{-1}\sigma$ no es la identidad, y verifica $F(\sigma) \subsetneq F(\alpha)$. En particular $f(\sigma) < f(\alpha)$.*

DEMOSTRACIÓN.

- Veamos en primer lugar que α no es la identidad. Se tiene

$$\alpha(a_1) = \beta\sigma\beta^{-1}\sigma(a_1) = \beta\sigma\beta^{-1}(a_2) = \beta\sigma(a_1) = \beta(a_2) = a_4.$$

Como $a_1 \in \operatorname{supp}(\tau_1)$ y $a_4 \in \operatorname{supp}(\tau_2)$, resulta que $a_1 \neq a_4$, ya que los ciclos τ_1 y τ_2 son disjuntos.

- Ahora probamos que $F(\sigma) \subseteq F(\alpha)$. Si $x \in F(\sigma)$, entonces $x \notin \text{supp}(\tau_1)$ y $x \notin \text{supp}(\tau_2)$, de donde

$$\sigma(x) = x, \qquad \beta^{-1}(x) = x, \qquad \beta(x) = x,$$

luego $\alpha(x) = x$ y $F(\sigma) \subseteq F(\alpha)$.

Veamos que $F(\sigma) \neq F(\alpha)$. Se tiene que $\sigma(a_2) = a_3 \neq a_2$. Sin embargo

$$\alpha(a_2) = \beta\sigma\beta^{-1}(a_3) = \beta\sigma(a_3) = \beta(a_1) = a_2,$$

por tanto $a_2 \in F(\alpha) \setminus F(\sigma)$.

■

Proposición 4.3.6 *Sea $n \geq 5$, y sea $\sigma = \tau_1 \cdots \tau_r \in S_n$ donde $\tau_1, \ldots, \tau_r$ son ciclos disjuntos dos a dos. Supongamos que*

$$\tau_1 = (a_1, a_2), \qquad \tau_2 = (a_3, a_4).$$

Sean

$$a_5 \in E_n \setminus \{a_1, a_2, a_3, a_4\}, \qquad y \qquad \beta = (a_1, a_2, a_5).$$

Entonces el elemento $\alpha = \beta\sigma\beta^{-1}\sigma$ no es la identidad, y $f(\sigma) < f(\alpha)$.

DEMOSTRACIÓN. Comprobamos en primer lugar que α no es la identidad.

$$\alpha(a_1) = \beta\sigma\beta^{-1}(a_2) = \beta\sigma(a_1) = \beta(a_2) = a_5$$

y al ser $a_1 \neq a_5$, se tiene que $\alpha \neq Id$. Para la segunda parte, veremos que

$$a_3, a_4 \in F(\alpha) \setminus F(\sigma) \text{ y } F(\sigma) \subset F(\alpha) \cup \{a_5\}.$$

Esto significa que hay dos elementos en $F(\alpha)$ que no están en $F(\sigma)$, y a lo sumo uno que está en $F(\sigma)$ y no en $F(\alpha)$. Así tendremos que $f(\sigma) < f(\alpha)$.

Como $\sigma(a_3) = a_4$ y $\sigma(a_4) = a_3$, se tiene que $a_3, a_4 \notin F(\sigma)$. Sin embargo

$$\alpha(a_3) = \beta\sigma\beta^{-1}(a_4) = \beta\sigma(a_4) = \beta(a_3) = a_3.$$

y

$$\alpha(a_4) = \beta\sigma\beta^{-1}(a_3) = \beta\sigma(a_3) = \beta(a_3) = a_4.$$

Sea $x \in F(\sigma)$, $x \neq a_5$. Entonces $x \notin \text{supp}(\tau_1)$. Por tanto, $x \neq a_1$, $x \neq a_2$, $x \neq a_5$. Así $x \notin \text{supp}(\beta)$, y por tanto

$$\beta(x) = x = \beta^{-1}(x).$$

Como $\sigma(x) = x$, resulta $\alpha(x) = x$.

■

Corolario 4.3.7 (Teorema de Abel) *Si $n \geq 5$, A_n es simple.*

DEMOSTRACIÓN. Sea N un subgrupo normal de A_n, $N \neq \{1\}$. Veremos que $N = A_n$. Para ello, basta probar, en virtud del Lema 4.3.2, que N contiene un ciclo de longitud 3. Sea $\sigma \in N$ tal que $f(\sigma)$ sea máximo entre los $f(\tau)$, $\tau \in N$, $\tau \neq 1$. Observemos que dicho σ existe ya que la función f está acotada superiormente:

$$f(\tau) = \text{card}\,(F(\tau)) < n \qquad \text{para cada} \qquad \tau \neq Id.$$

Vamos a demostrar, utilizando las proposiciones anteriores, que σ es el ciclo de longitud 3 que buscamos.

Por la Proposición 4.2.12, podemos escribir

$$\sigma = \tau_1 \cdots \tau_r$$

donde $\tau_1, \ldots, \tau_r$ son ciclos disjuntos dos a dos, diferentes de la identidad. Veremos que $r = 1$ y que $\sigma = \tau_1$ tiene longitud 3.

Afirmamos en primer lugar que long $(\tau_i) < 4$ para todo $1 \leq i \leq r$, ya que en caso contrario podemos suponer que long $(\tau_1) \geq 4$, y por la Proposición 4.3.4 existe β ciclo de longitud 3, que por Corolario 4.2.28 pertenece a A_n, tal que

$$\alpha = \beta^{-1}\sigma^{-1}\beta \neq Id$$

y $f(\sigma) < f(\alpha)$.

Pero por hipótesis N es un subgrupo normal de A_n, y $\sigma^{-1} \in N$, de donde se tiene que $\beta^{-1}\sigma^{-1}\beta \in N$, es decir

$$\alpha \in N \qquad \text{con} \qquad f(\sigma) < f(\alpha),$$

y esto contradice la elección de σ.

Veamos ahora que a lo sumo hay un τ_i que es transposición. Si hubiese más, por la Proposición 4.3.6, existe $\beta \in A_n$ tal que

$$\alpha = \beta^{-1}\sigma^{-1}\beta \neq Id$$

y $f(\sigma) < f(\alpha)$. En este caso, por el mismo razonamiento anterior, tenemos que $\alpha \in N$ con $f(\sigma) < f(\alpha)$, en contra de la elección de σ.

Nuestro siguiente paso es comprobar que de hecho ningún τ_i es trasposición. De lo contrario por lo anterior, exactamente uno lo sería. Podríamos suponer τ_1. Tendríamos entonces

$$\sigma = \tau_1 \cdots \tau_r,$$

siendo τ_1 una trasposición y $\tau_2, \ldots, \tau_r$ son ciclos de longitud 3, que por Corolario 4.2.28, pertenecen a A_n. Pero entonces

$$\tau_1 = \sigma\tau_r^{-1} \cdots \tau_2^{-1} \in A_n,$$

en contradicción con el hecho de que $\varepsilon(\tau_1) = -1$.

Así hemos obtenido que

$$\sigma = \tau_1 \cdots \tau_r$$

donde cada τ_i es de longitud 3.

Si $r \neq 1$, por la Proposición 4.3.5 existe $\beta \in A_n$ tal que

$$\alpha = \beta\sigma\beta^{-1} \neq Id, \qquad f(\sigma) < f(\alpha).$$

Argumentando como antes

$$\alpha \in N, \qquad \alpha \neq Id, \qquad f(\sigma) < f(\alpha),$$

en contra de la elección de σ.

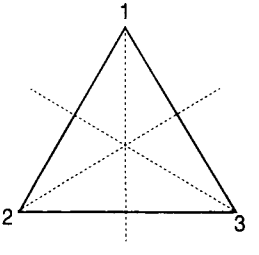
Por lo tanto $r = 1$ y $\sigma = \tau_1$ es un ciclo de longitud 3, como queríamos demostrar.

■

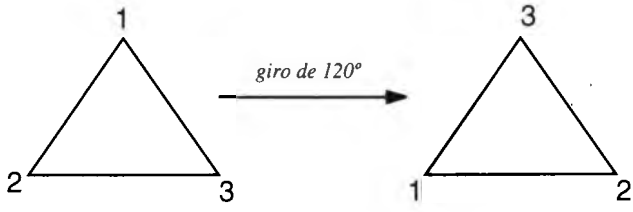
4.4. El grupo diédrico

En esta sección, aplicando las técnicas desarrolladas en las secciones anteriores, expresaremos el grupo de las simetrías de un polígono regular de n lados, también llamado grupo diédrico n-ésimo, en términos de generadores e identidades satisfechas por estos ("relaciones"). Vamos a establecer, de manera constructiva, cuál es el aspecto de este grupo en varios casos concretos, e induciremos la forma general de dicho grupo.

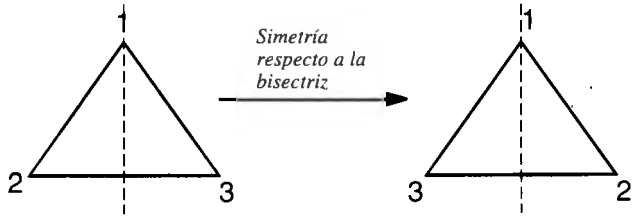
Para ello, empecemos con el polígono regular más sencillo: el triángulo. Una simple inspección hace manifiesto que los únicos movimientos posibles son simetrías respecto a las bisectrices y rotaciones respecto al circuncentro (de ángulos fijados).



De hecho, las rotaciones posibles se obtienen por iteración de la rotación de ángulo $2\pi/3$, que denotamos por ρ.



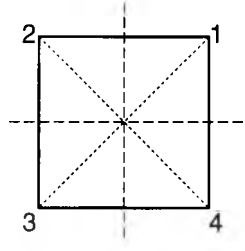
Usando dichas rotaciones, es obvio que las simetrías respecto a cualquiera de los ejes se obtiene componiendo la simetría, denotada σ,



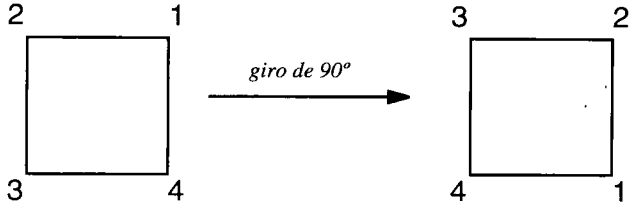
con rotaciones adecuadas. Claramente, todo movimiento se obtiene por composición de la rotación ρ y la simetría σ. Asimismo, es fácil ver que las únicas relaciones entre ellas son:

$$\rho^3 = Id, \quad \sigma^2 = Id, \quad \sigma\rho = \rho^{-1}\sigma.$$

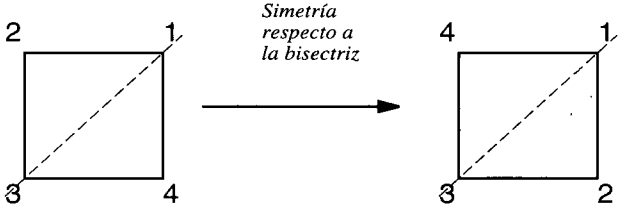
El siguiente caso es el del cuadrado. En este caso, los únicos movimientos posibles son simetrías respecto a los apotemas y las bisectrices, así como rotaciones respecto al circuncentro (de ángulos fijados).



De hecho, las rotaciones posibles se obtienen por iteración de la rotación de ángulo $\pi/2$, que denotamos por ρ.

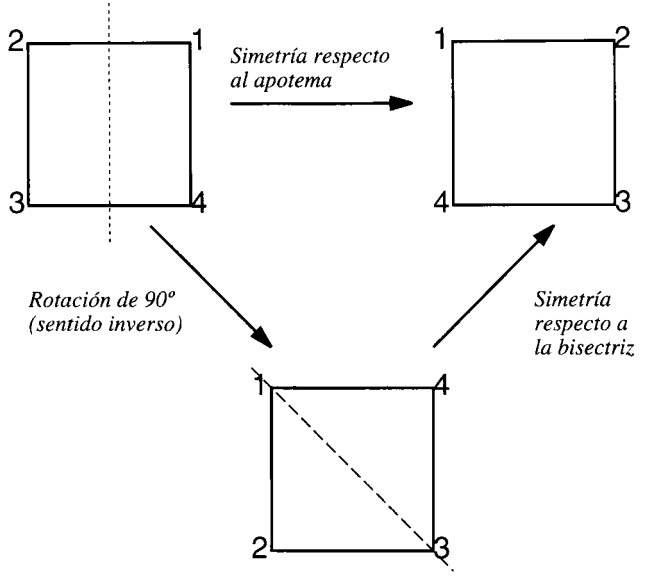


Usando dichas rotaciones, es obvio que las simetrías respecto a cualquiera de los ejes se obtiene componiendo las simetrías, denotadas respectivamente σ,



y τ,

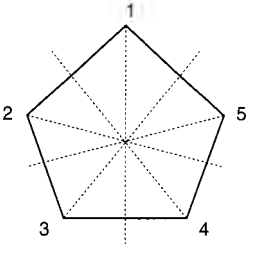
con rotaciones adecuadas. En este caso, de hecho, la simetría τ se puede obtener por composición de una rotación con la simetría σ; concretamente, $\tau = \sigma\rho^{-1}$, como se observa a la siguiente figura



Por tanto, todo movimiento se obtiene por composición de la rotación ρ y la simetría σ. Asimismo, es fácil ver que las únicas relaciones entre ellas son:

$$\rho^4 = Id, \quad \sigma^2 = Id, \quad \sigma\rho = \rho^{-1}\sigma.$$

El siguiente caso es el del pentágono. Como en el caso del triángulo, los únicos movimientos posibles son simetrías respecto a las bisectrices, así como rotaciones respecto al circuncentro (de ángulos fijados).



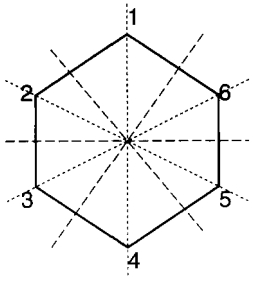
De hecho, las rotaciones posibles se obtienen por iteración de la rotación de ángulo $2\pi/5$, que denotamos por ρ.

Usando dichas rotaciones, es obvio que las simetrías respecto a cualquiera de los ejes se obtiene componiendo la simetría, denotada σ,

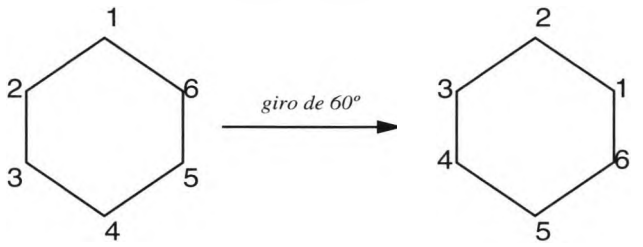
con rotaciones adecuadas. Claramente, todo movimiento se obtiene por composición de la rotación ρ y la simetría σ. Asimismo, es fácil ver que las únicas relaciones entre ellas son:

$$\rho^5 = Id, \quad \sigma^2 = Id, \quad \sigma\rho = \rho^{-1}\sigma.$$

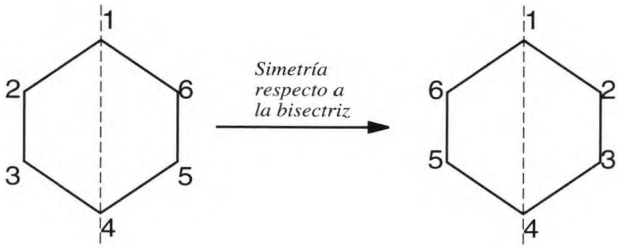
Finalmente, consideremos el caso del hexágono. Como en el caso del cuadrado, los únicos movimientos posibles son simetrías respecto a las bisectrices y los apotemas, así como rotaciones respecto al circuncentro (de ángulos fijados).



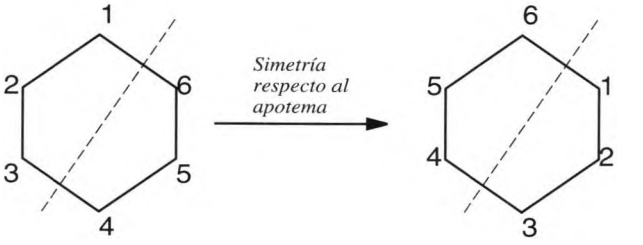
De hecho, las rotaciones posibles se obtienen por iteración de la rotación de ángulo $\pi/3$, que denotamos por ρ.



Usando dichas rotaciones, es obvio que las simetrías respecto a cualquiera de los ejes se obtiene componiendo las simetrías, denotadas respectivamente σ,



y τ,



con rotaciones adecuadas. En este caso, de hecho, la simetría τ se puede obtener por composición de una rotación con la simetría σ, de manera análoga al caso del cuadrado, obteniéndose nuevamente la relación $\tau = \sigma\rho^{-1}$. Por tanto, todo movimiento se obtiene por composición de la rotación ρ y la simetría σ. Asimismo, es fácil ver que las únicas relaciones entre ellas son:

$$\rho^6 = Id, \quad \sigma^2 = Id, \quad \sigma\rho = \rho^{-1}\sigma.$$

Para extender los resultados obtenidos al caso general, la manera más efectiva consiste en fijar un valor para cada vértice del polígono dado, como se

ha hecho en las figuras anteriores, e identificar cada movimiento con la permutación de ese conjunto que le corresponda. Así, para el triángulo tenemos, en S_3:

$$\rho = (1,2,3), \quad \sigma = (2,3),$$

para el cuadrado tenemos, en S_4:

$$\rho = (1,2,3,4), \quad \sigma = (2,4),$$

para el pentágono tenemos, en S_5:

$$\rho = (1,2,3,4,5), \quad \sigma = (2,5)(3,4),$$

y para el hexágono tenemos, en S_6:

$$\rho = (1,2,3,4,5,6), \quad \sigma = (2,6)(3,5).$$

A partir de estas representaciones, no es difícil obtener la expresión general para los generadores del grupo diédrico n-ésimo.

Definición 4.4.1 *Sea $n \geq 3$, y sea S_n el grupo de permutaciones. Se denomina grupo diédrico D_n al subgrupo de S_n generado por $a = (1,2,3,\ldots,n)$ y*

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & i & \ldots & n-1 & n \\ 1 & n & n-1 & n-2 & \ldots & n+2-i & \ldots & 3 & 2 \end{pmatrix} = \\ = \prod_{2 \leq i < r} (i, n+2-i),$$

donde

$$r = \begin{cases} \frac{n}{2} & si \quad n \text{ es par} \\ \frac{n+1}{2} & si \quad n \text{ es impar.} \end{cases}$$

Finalmente, vamos a probar que cualquier grupo de $2n$ elementos con dos generadores satisfaciendo un conjunto concreto de relaciones es isomorfo al grupo diédrico n-ésimo.

Teorema 4.4.2 *Para cada $n \geq 3$, el grupo diédrico D_n es un grupo de orden $2n$, con 2 generadores a, b satisfaciendo:*

1. $a^n = 1$; $b^2 = 1$; $a^k \neq 1$ *si* $0 < k < n$.
2. $ba = a^{-1}b$.

Más aún, todo grupo con 2 generadores satisfaciendo estas relaciones es isomorfo a D_n.

DEMOSTRACIÓN. Es fácil comprobar que los elementos a y b de la Definición 4.4.1 satisfacen (1) y (2). Por tanto, los elementos de D_n son de la forma $a^i b^j$, con $0 \leq i < n$, $j = 0, 1$. Observando como actúan sobre los elementos $1, 2 \in E_n$, es fácil ver que los elementos $a^i b^j$, con $0 \leq i < n$, $j = 0, 1$ son permutaciones distintas de E_n, de donde $o(D_n) = 2n$.

Para $n \geq 3$, sea G un grupo con generadores a, b satisfaciendo (1) y (2). Como todo elemento x del grupo tiene una expresión de la forma

$$x = a^{m_1} b^{m_2} a^{m_3} \cdots b^{m_k} \quad (m_i \in \mathbb{Z}),$$

usando (1) y (2) repetidas veces se reduce x a la expresión $a^i b^j$, $0 \leq i < n$, $j = 0, 1$. Si denotamos los generadores de D_n como a_1, b_1, es claro que la aplicación

$$\begin{array}{rccc} f: & D_n & \longrightarrow & G \\ & a_1 & \longmapsto & a \\ & b_1 & \longmapsto & b \end{array}$$

define un epimorfismo de grupos.

Veamos que f es un monomorfismo. Para ello, sea $a_1^i b_1^j \in \ker(f)$. Si $j = 1$, entonces $a^i b = 1$, de donde $a^i = b^{-1} = b$ por la relación (1). Por la relación (2) tenemos $a^{i+1} = a^i a = ba = a^{-1}b = a^{-1}a^i = a^{i-1}$. Por tanto, $a^2 = 1$, lo que es imposible, ya que $n \geq 3$ y a satisface (1). Así, $j = 0$, de donde $a^i = 1$, y como $0 \leq i < n$, concluimos que $i = 0$, ya que a satisface (1). Así, f es un monomorfismo, y en consecuencia un isomorfismo.

■

4.5. Ejercicios

1. Descomponed en producto de ciclos disjuntos las permutaciones siguientes:

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix},$$

$$d = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 & 2 & 1 \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 2 & 1 & 3 & 4 & 6 \end{pmatrix}.$$

2. Dadas las siguientes permutaciones

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, i = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix},$$

$$o = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \; d = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$

a) Efectuad el producto de las permutaciones, siempre que sea posible, designadas por una vocal por las designadas por una consonante, expresándolas previamente como producto de ciclos disjuntos.

b) Determinad las inversas de dichas permutaciones.

c) Hallad el índice de dichas permutaciones.

3. Dada la permutación $\sigma \in S_7$ siguiente

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 7 & 4 & 6 & 2 & 3 \end{pmatrix},$$

a) Descomponed en producto de ciclos disjuntos las permutaciones σ, σ^2, σ^{-1}.

b) Calculad el orden de σ y de σ^2.

4. En el grupo simétrico S_7 calculad los siguientes elementos

$$(4,5,6)^{1994}; \quad (1,2,4)^{-382}; \quad (4,2,1,6,7)^{1492}; \quad (5,1,2)^{10835}.$$

5. Probad que los siguientes subconjuntos de S_4 son subgrupos

a) $\{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

b) $\{I, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$.

c) $\{I, (1,3), (2,4), (1,3)(2,4), (1,2,3,4), (1,2)(3,4), (1,4,3,2), (1,4)(2,3)\}$.

6. Demostrad que el subgrupo del apartado (*a*) del ejercicio anterior es un subgrupo normal de A_4.

7. Demostrad que el grupo A_4 tiene orden 12 y no posee ningún subgrupo de orden 6. ¿Existe algún homomorfismo inyectivo de S_3 en A_4?

8. Escribid todos los elementos de los grupos alternados A_3 y A_4.

9. Demostrad que

a) $Z(S_n) = \{1\}$ para $n \geq 3$.

b) $Z(A_n) = \{1\}$ para $n \geq 4$.

10. Sea $n \geq 2$ un número natural. Demostrad que son equivalentes las siguientes afirmaciones

a) A_n es simple.

b) $n \neq 4$.

11. Sea G un grupo finito, y sea H un subgrupo de G que no contiene ningún subgrupo normal no trivial de G. Probad que G es isomorfo a un subgrupo del grupo de permutaciones del conjunto G/H.

Capítulo 5

Teoremas de Sylow

En este capítulo, usando como instrumento, las acciones de grupos sobre conjuntos, vamos a probar los Teorema de Sylow, que garantiza la existencia de ciertos subgrupos de un grupo finito dado, así como el número posible de tales subgrupos. Estos teoremas son uno de los instrumentos básicos para conocer la estructura de un grupo, en base a su cardinalidad.

5.1. G-conjuntos

Definición 5.1.1 *Sean Ω un conjunto y G un grupo. Decimos que G actúa sobre Ω por la izquierda, si existe una aplicación*

$$\begin{array}{ccc} G \times \Omega & \longrightarrow & \Omega \\ (g, w) & \longmapsto & g \perp w \end{array}$$

que verifica:

1. $g_1 \perp (g_2 \perp w) = (g_1 g_2) \perp w, \qquad \forall\, g_1, g_2 \in G, \forall\, w \in \Omega.$
2. $1 \perp w = w, \qquad \forall\, w \in \Omega.$

También se dice que Ω es un G-conjunto. Decimos que la acción es propia si para todo $w \in \Omega$, $g \perp w = w$, entonces $g = 1$.

Lema 5.1.2 *Sean Ω un conjunto y G un grupo. Son equivalentes:*

1. *Ω es un G-conjunto.*
2. *Existe un homomorfismo de grupos $\phi : G \longrightarrow S(\Omega)$, donde $S(\Omega)$ representa al conjunto de las aplicaciones biyectivas en Ω.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2) : Si Ω es un G-conjunto entonces podemos considerar la aplicación

$$\begin{array}{rccccc} \phi: & G & \longrightarrow & S(\Omega) & & \\ & g & \longmapsto & \phi_g : \Omega & \longrightarrow & \Omega \\ & & & w & \longmapsto & g\perp w, \end{array}$$

donde $g\perp w$ está definido por la acción de G sobre Ω. Se tiene que:

- ϕ_g es una aplicación biyectiva en Ω con inversa $\phi_{g^{-1}}$.
- ϕ es un homomorfismo de grupos, ya que para todo $w \in \Omega$ se tiene

$$\phi_{g_1g_2}(w) = (g_1g_2)\perp w = g_1\perp(g_2\perp w) = \phi_{g_1}(g_2\perp w) = \phi_{g_1}\phi_{g_2}(w).$$

Por tanto,

$$\phi_{g_1g_2} = \phi_{g_1}\phi_{g_2}, \qquad \text{para todo} \qquad g_1,\, g_2 \in G.$$

(2) $\Longrightarrow$ (1) : Si definimos $g\perp w = \phi(g)(w)$, se tiene que la aplicación

$$\begin{array}{ccc} G\times\Omega & \longrightarrow & \Omega \\ (g,w) & \longmapsto & g\perp w, \end{array}$$

define una acción de G sobre Ω ya que:

(1) Para todo $g_1,\, g_2 \in G$ y para todo $w \in \Omega$,

$$(g_1g_2)\perp w = \phi(g_1g_2)(w) = (\phi(g_1)\phi(g_2))(w) =$$

$$= \phi(g_1)(\phi(g_2)(w)) = \phi(g_1)(g_2\perp w) = g_1\perp(g_2\perp w).$$

(2) Para todo $w \in \Omega$,

$$1\perp w = \phi(1)(w) = Id(w) = w.$$

■

Llamaremos núcleo de la acción al núcleo del morfismo ϕ, y diremos que la acción es fiel si ϕ es inyectivo.

Ejemplos 5.1.3 *1. Para un número natural n, consideremos el conjunto $E_n = \{1,\ldots,n\}$. La aplicación*

$$\begin{array}{ccc} S_n\times E_n & \longrightarrow & E_n \\ (\sigma,i) & \longmapsto & \sigma(i), \end{array}$$

es una acción del grupo simétrico S_n sobre el conjunto E_n, y el homomorfismo asociado $S_n \longrightarrow S(E_n)$ es la identidad.

Más generalmente, si Ω es un conjunto arbitrario y G es un subgrupo del grupo simétrico $S(\Omega)$, entonces la aplicación

$$\begin{array}{rcl} \phi : G & \to & S(\Omega) \\ \sigma & \longmapsto & \sigma \end{array}$$

induce una acción fiel de G sobre Ω.

2. *Sea G un grupo y sea $\Omega = G$. La aplicación*

$$\begin{array}{rcl} G \times \Omega & \longrightarrow & \Omega \\ (g, w) & \longmapsto & gw \end{array}$$

es una acción de G sobre sí mismo. Se denomina acción de G sobre sí mismo por traslaciones por la izquierda. Nótese que es fiel ya que, si $g \in G$ satisface $gw = w$ para todo $w \in \Omega$, en particular para $w = 1$ tenemos $g1 = 1$. Por tanto $g = 1$.

3. *Sean G un grupo, H un subgrupo de G y Ω el conjunto G/H de las clases laterales por la izquierda módulo H. La aplicación*

$$\begin{array}{rcl} G \times \Omega & \longrightarrow & \Omega \\ (g, xH) & \longmapsto & gxH \end{array}$$

es una acción de G sobre Ω, que también se llama acción por traslaciones por la izquierda de G sobre G/H. Cuando $H = 1$ tenemos la acción del ejemplo anterior.

4. *Dado un grupo G, la aplicación*

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gxg^{-1} \end{array}$$

es una acción de G sobre sí mismo, denominada acción de G sobre sí mismo por conjugación. Más generalmente, si H y N son subgrupos de G y N es normal en G, la conjugación induce una acción de H sobre N que se denomina acción de H sobre N por conjugación.

Definición 5.1.4 *Dados Ω, Ω' G-conjuntos, definimos un morfismo de G-conjuntos como una aplicación*

$$f : (\Omega, \perp) \longrightarrow (\Omega', *)$$

tal que $g * f(w) = f(g \perp w)$, para todo $g \in G$ y para todo $w \in \Omega$.

Observación 5.1.5 *Si f es un morfismo entre los G-conjuntos Ω y Ω', se tiene que $f(\Omega)$ es un G-conjunto. Vamos a razonarlo:*

Como $g * f(w) = f(g \perp w)$, se tiene que $g * f(w) \in f(\Omega)$. Entonces tiene sentido la aplicación

$$\begin{array}{rcl} G \times f(\Omega) & \longrightarrow & f(\Omega) \\ (g, f(w)) & \longmapsto & g * f(w). \end{array}$$

Se comprueba que dicha aplicación es una acción de G sobre $f(\Omega)$.

Supongamos que tenemos definido un morfismo f entre los G-conjuntos Ω y Ω'. Consideremos la siguiente relación en Ω: dados w_1, $w_2 \in \Omega$, diremos que

$$w_1 \mathcal{R} w_2 \Longleftrightarrow f(w_1) = f(w_2).$$

$\mathcal{R}$ define una relación de equivalencia sobre Ω. Consideramos el conjunto cociente $\Omega/\mathcal{R}$, definido sobre Ω por la relación $\mathcal{R}$.

Veamos que $\Omega/\mathcal{R}$ es un G-conjunto. Para ello definimos la aplicación

$$\begin{array}{rcl} G \times \Omega/\mathcal{R} & \longrightarrow & \Omega/\mathcal{R} \\ (g, \overline{w}) & \longmapsto & \overline{g \perp w}. \end{array}$$

- Observamos que está bien definida: Si $\overline{w}_1 = \overline{w}_2$ entonces $f(w_1) = f(w_2)$. Por tanto,

  $$f(g \perp w_1) = g * f(w_1) = g * f(w_2) = f(g \perp w_1).$$

  Así, $\overline{g \perp w_1} = \overline{g \perp w_2}$.

- Ahora es elemental comprobar que esta aplicación es una acción de G sobre $\Omega/\mathcal{R}$.

Finalmente veamos que los G-conjuntos $\Omega/\mathcal{R}$ y $f(\Omega)$ son isomorfos, es decir existe una biyección de G-conjuntos entre ellos. Para ello, consideremos la aplicación

$$\begin{array}{rcl} \widehat{f} : \Omega/\mathcal{R} & \longrightarrow & f(\Omega) \\ \overline{w} & \longmapsto & f(w). \end{array}$$

Es elemental comprobar que $\widehat{f}$ está bien definida y es biyectiva. Veamos que $\widehat{f}$ es un morfismo de G-conjuntos, ya que

$$\widehat{f}(g \perp \overline{w}) = \widehat{f}(\overline{g \perp w}) = f(g \perp w) = g * f(w) = g * \widehat{f}(\overline{w}).$$

Observemos que este resultado es un análogo del Primer Teorema de Isomorfía para G-conjuntos. Este resultado será básico para desarrollar nuestras técnicas de contabilidad. Vamos a ver ahora cómo se aplica a una acción abstracta de uso común.

Sean G un grupo y Ω un G-conjunto. Fijado $w \in \Omega$, consideremos el morfismo de G-conjuntos definido como

$$\begin{aligned} \varphi : G &\longrightarrow \Omega \\ g &\longmapsto g \perp w. \end{aligned}$$

Definición 5.1.6 *Dado $w \in \Omega$, con la notación anterior, el conjunto*

$$\varphi(G) = \{g \perp w : g \in G\}$$

se denota $\mathcal{O}_w$ y se denomina órbita de w por G.

Consideremos en G la relación

$$g_1 \mathcal{R} g_2 \Longleftrightarrow \varphi(g_1) = \varphi(g_2).$$

Observemos que

$$\varphi(g_1) = \varphi(g_2) \Longleftrightarrow g_1 \perp w = g_2 \perp w \Longleftrightarrow g_2^{-1} \perp (g_1 \perp w) = g_2^{-1} \perp (g_2 \perp w) \Longleftrightarrow$$

$$\Longleftrightarrow \left(g_2^{-1} g_1\right) \perp w = \left(g_2^{-1} g_2\right) \perp w \Longleftrightarrow \left(g_2^{-1} g_1\right) \perp w = w.$$

En este caso tenemos que el conjunto

$$H_w = \{g \in G : g \perp w = w\}$$

es un subgrupo de G, no necesariamente normal, que define la relación anterior, es decir

$$g_1 \mathcal{R} g_2 \Longleftrightarrow g_1 g_2^{-1} \in H_w.$$

Por las observaciones anteriores, podemos afirmar que

$$G/H_w \cong O_w \text{ como } G\text{-conjuntos .}$$

H_w es el llamado estabilizador (o grupo de isotropía) de w en G.

Definición 5.1.7 *Sea un grupo G actuando sobre un conjunto Ω. Diremos que la acción es transitiva, o que G actúa transitivamente en Ω, si todos los elementos están sobre la misma órbita.*

Ejemplos 5.1.8 *1. Sea G el subgrupo cíclico de S_6 generado por la permutación $\sigma = (1,2,3)(4,5)$ y consideramos la acción $G \times E_6 \longrightarrow E_6$ definida en el Ejemplo 5.1.3(1). Entonces, las órbitas son $\{1,2,3\}$, $\{4,5\}$ y $\{6\}$, el único punto fijo de E_6 es el 6, y los estabilizadores son*

$$H_1 = H_2 = H_3 = \left\{1, \sigma^3\right\}, \quad H_4 = H_5 = \left\{1, \sigma^2, \sigma^4\right\}, \quad H_6 = G.$$

2. La acción natural del subgrupo

$$V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

de S_4 sobre E_4 es transitiva, y cada elemento de E_4 tiene estabilizador trivial.

3. La acción de un grupo G sobre sí mismo por traslaciones a la izquierda es transitiva, pues cada ecuación $aX = b$ tiene solución única en G. También lo es la acción de G en G/H por traslaciones por la izquierda.

Lema 5.1.9 *Sean G un grupo y Ω un G-conjunto. Las órbitas de los elementos de Ω por G forman una partición de Ω.*

DEMOSTRACIÓN. En primer lugar veamos que $\Omega = \bigcup_{w\in\Omega} \mathcal{O}_w$.

Por definición de órbita, se tiene que $\mathcal{O}_w \subset \Omega$. Para la otra inclusión basta tener en cuenta que si Ω es un G-conjunto se tiene que $w = 1 \perp w$ para todo $w \in \Omega$.

Veamos a continuación que las órbitas son disjuntas o coinciden. Para ello, sean $\mathcal{O}_w$, $\mathcal{O}_{w'}$, y supongamos que existe $g \in \mathcal{O}_w \cap \mathcal{O}_{w'}$. Entonces, para g_1, $g_2 \in G$ y $w, w' \in \Omega$, se tiene

$$g = g_1 \perp w = g_2 \perp w'.$$

Así

$$\left(g_2^{-1} g_1\right) \perp w = w', \qquad \left(g_1^{-1} g_2\right) \perp w' = w.$$

Por tanto, para todo $h \in G$, se tiene

$$h \perp w = \left(h g_1^{-1} g_2\right) \perp w',$$

de donde $\mathcal{O}_w \subseteq \mathcal{O}_{w'}$, y recíprocamente

$$h \perp w' = \left(h g_2^{-1} g_1\right) \perp w,$$

de donde $\mathcal{O}_{w'} \subseteq \mathcal{O}_w$. Por tanto se tiene $\mathcal{O}_w = \mathcal{O}'_w$.

■

Ahora, en cada órbita escogemos un elemento arbitrario. La colección así obtenida, que denotamos por Y, se denomina Sistema de representantes de las órbitas de G.

Usando el Lema 5.1.9, se tiene el siguiente resultado que es la clave de las demostraciones de los Teoremas de Sylow.

Corolario 5.1.10 (Fórmula de sumación de órbitas) *Si Ω es un G-conjunto finito e Y es un sistema de representantes de las órbitas, entonces*

$$\operatorname{card}(\Omega) = \sum_{w \in Y} [G : H_w].$$

5.2. Ecuación de las órbitas

Comenzamos esta sección dando la definición de dos subgrupos que van a tener gran interés en el resto del capítulo.

Definición 5.2.1 *Dado un grupo G, definimos su centro como el subconjunto*

$$Z(G) = \{h \in G : hg = gh, \forall g \in G\}.$$

Es fácil comprobar que $Z(G)$ es subgrupo normal de G. Además G es abeliano si y sólo si $Z(G) = G$.

Definición 5.2.2 *Si G es un grupo, se define el centralizador en G de un elemento $x \in G$ como el subconjunto*

$$C_G(x) = \{g \in G : gx = xg\}.$$

Se tiene que:

1. $C_G(x)$ es un subgrupo de G.
2. $Z(G) = \bigcap_{x \in G} C_G(x)$.
3. $x \in Z(G) \iff C_G(x) = G$.

La demostración se propone como ejercicio.

Sea G un grupo y tomamos la acción de G sobre sí mismo por conjugación, que hemos visto en el Ejemplo 5.1.3(4),

$$\begin{array}{rcl} G \times \Omega & \longrightarrow & \Omega \\ (g, w) & \longmapsto & gwg^{-1} \end{array}$$

donde $\Omega = G$. Se tiene

$$\text{card}\,(\mathcal{O}_w) = 1 \iff gwg^{-1} = w \qquad \text{para todo} \qquad g \in G,$$

esto es

$$\text{card}\,(\mathcal{O}_w) = 1 \iff w \in Z(G).$$

Asimismo, en el caso de G actuando sobre sí mismo por conjugación tenemos que

$$H_w = \{g \in G : \ gw = wg\}.$$

Es decir $H_w = C_G(w)$. Por tanto, en virtud del Lema 5.1.9, tenemos el siguiente resultado.

Proposición 5.2.3 *Sea G un grupo finito, sea Y un sistema de representantes de las órbitas de G por conjugación. Entonces*

$$o(G) = o(Z(G)) + \sum_{w \in Y \setminus Z(G)} [G : C_G(w)].$$

DEMOSTRACIÓN. Dado que las clases de conjugación forman una partición de G, tenemos que

$$G = \bigcup_{w \in Y} \mathcal{O}_w.$$

Por tanto,

$$o(G) = \sum_{w \in Y} \text{card}(\mathcal{O}_w) = \sum_{w \in Y \cap Z(G)} \text{card}\,(\mathcal{O}_w) + \sum_{w \in Y \setminus Z(G)} \text{card}\,(\mathcal{O}_w).$$

Pero si $w \in Y \cap Z(G)$, tendremos que $w \in Z(G)$, es decir $wg = gw$ para todo $g \in G$. Luego $C_G(w) = G$, y en tal caso, se tiene que

$$\text{card}\,(\mathcal{O}_w) = [G : C_G(w)] = 1.$$

De este modo

$$\sum_{w \in Y \cap Z(G)} \text{card}\,(\mathcal{O}_w) = \text{card}(Y \cap Z(G)).$$

Vamos a demostrar que $Z(G) \subseteq Y$. Para ello, consideremos $w, w' \in Z(G)$ tales que $w \neq w'$, entonces veamos que $\mathcal{O}_w \neq \mathcal{O}_{w'}$.

Supongamos que $\mathcal{O}_w = \mathcal{O}_{w'}$, entonces $w' \in \mathcal{O}_{w'} = O_w$. Por tanto $w' = gwg^{-1}$ para algún $g \in G$. Así, como $w \in Z(G)$, se tiene

$$w'g = gw = wg,$$

de donde podemos afirmar que $w = w'$, contradiciendo nuestras hipótesis. Por tanto $Z(G) \subseteq Y$, de donde

$$\text{card}(Y \cap Z(G)) = \text{card}(Z(G)).$$

Así podemos afirmar que

$$o(G) = o(Z(G)) + \sum_{w \in Y \setminus Z(G)} [G : C_G(w)].$$

■

De la ecuación de clases de conjugación se pueden deducir algunas propiedades de los grupos cuyo orden es una potencia de un número primo.

Definición 5.2.4 *Sea p un número primo. Se dice que G es un p-grupo si $o(G) = p^m$ para algún $m \in \mathbb{N}$.*

Corolario 5.2.5 *Sea G un p-grupo. Entonces $o(Z(G)) > 1$. Además, $o(Z(G)) \neq p^{m-1}$.*

DEMOSTRACIÓN. Como hemos observado anteriormente, para todo $w \notin Z(G)$ se tiene $1 \neq [G : H_w]$, y por el Teorema de Lagrange $[G : H_w]$ divide a p^m. Entonces, por la ecuación de las clases de conjugación, tenemos que

$$o(G) = o(Z(G)) + lp,$$

donde lp representa a un múltiplo de p. Si $o(Z(G)) = 1$ entonces se tendría que $p^m - 1$ es un múltiplo de p, que es absurdo.

Para la segunda afirmación, si $o(G) = p^m$, como $Z(G)$ es subgrupo de G, por el Teorema de Lagrange, $o(Z(G))$ divide a p^m. Por tanto existe $1 \leq h \leq m$ tal que $o(Z(G)) = p^h$.

Si $o(Z(G)) = p^{m-1}$, entonces

$$\frac{o(G)}{o(Z(G))} = \frac{p^m}{p^{m-1}} = p,$$

de donde podemos afirmar que $G/Z(G)$ es un grupo cíclico, y como consecuencia se tiene que G es un grupo abeliano. Por tanto $Z(G) = G$, lo que nos lleva a afirmar que $p^{m-1} = p^m$, que es absurdo. Por tanto $o(Z(G)) \neq p^{m-1}$.

■

Corolario 5.2.6 *Si p es un número primo y G un grupo de orden p^2, entonces G es abeliano. De hecho G es isomorfo a $\mathbb{Z}/p^2\mathbb{Z}$ o a $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.*

DEMOSTRACIÓN. Por el Teorema de Lagrange, el orden de $Z(G)$ es un divisor de p^2. Por tanto sólo puede ser 1, p o p^2. Como $o(Z(G)) \neq 1$ y $o(Z(G)) \neq p$ por el Corolario 5.2.5, entonces ha de ser $o(Z(G)) = p^2$, de modo que $Z(G) = G$. Por tanto G es un grupo abeliano.

Por el Teorema de Estructura de grupos abelianos finitamente generados, como p^2 y $p \cdot p$ son las únicas descomposiciones en factores de p, se deduce que

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \qquad \text{ó} \qquad G \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}).$$

Claramente estos dos grupos no son isomorfos entre sí, ya que $G \cong \mathbb{Z}/p^2\mathbb{Z}$ es cíclico, mientras que $G \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ no es cíclico. Así pues, salvo isomorfismo, existen exactamente dos grupos de orden p^2.

■

Corolario 5.2.7 *Si G es un p-grupo, con $o(G) > p$, entonces G no es simple.*

DEMOSTRACIÓN. Pueden ocurrir dos casos:

1. Si G no es abeliano, entonces $Z(G) \neq G$. Por el Corolario 5.2.5 tenemos que $Z(G) \neq \{1\}$, y al ser $Z(G)$ un subgrupo normal de G ya tendríamos el resultado.

2. Si G es abeliano, entonces pueden ocurrir dos casos:

   a) Para todo $a \in G \setminus \{1\}$, se tiene $o(a) \neq p^m$. Entonces consideramos el subgrupo $H = \langle a \rangle$, que es normal, pues G es abeliano y $\{1\} \neq H \neq G$.

   b) Si existe $a \in G \setminus \{1\}$ tal que $o(a) = p^m$, entonces G es cíclico, y tiene un subgrupo para cada divisor de p^m. Como G es abeliano, todo subgrupo es normal, de donde hemos acabado.

■

5.3. Teoremas de Sylow

Ahora utilizaremos técnicas de acciones de grupos sobre conjuntos para probar tres resultados muy útiles en el estudio de la estructura de un grupo finito.

Teorema 5.3.1 (Primer Teorema de Sylow)
Sea G un grupo tal que $o(G) = mp^n$, con p primo y $\text{mcd}(p, m) = 1$. Entonces, para cada $1 \leq h \leq n$, existe un subgrupo de G de orden p^h.

DEMOSTRACIÓN. Consideremos los subconjuntos de G cuyo cardinal sea p^h, y sea A el conjunto de tales subconjuntos, es decir

$$A = \{C \subset G : \text{card}(C) = p^h\}.$$

Consideremos la acción de G sobre A definida por

$$\begin{array}{ccc} G \times A & \longrightarrow & A \\ (g, C) & \longmapsto & gC. \end{array}$$

Claramente, está bien definida, y con ello A es un G-conjunto. Como G es finito, y A es un subconjunto del conjunto de las partes de G, se tiene que $\text{card}(A) < 2^{o(G)}$, de donde A es finito.

Como

$$\text{card}(A) = \binom{p^n m}{p^h} = \frac{p^n m(p^n m - 1) \cdots (p^n m - p^h + 1)}{p^h(p^h - 1) \cdots (p^h - p^h + 1)} =$$

$$= p^{n-h} \frac{m(p^n m - 1) \cdots (p^n m - p^h + 1)}{(p^h - 1) \cdots (p^h - p^h + 1)},$$

podemos afirmar que p^{n-h} divide a $\text{card}(A)$. Más aún, p^{n-h+1} no divide a $\text{card}(A)$, ya que

$$\binom{p^h\,(p^{n-h}m)}{p^h} = \binom{p^n m}{p^h},$$

y las máximas potencias de p que dividen a $\binom{p^n m}{p^h}$ y $p^{n-h}m$, coinciden, como pueden verse en la lista de problemas.

Por el Corolario 5.1.10 se tiene

$$\text{card}(A) = \sum_{C \in A} [G : H_C],$$

donde $H_C = \{g \in G : gC = C\}$. Si $\text{card}(H_C) = p^k m'$, entonces se tiene que $p^k m'$ es divisor de $p^n m$, ya que H_C es un subgrupo de G.

Por tanto existe $C \in A$ tal que p^{n-h+1} no divide a $[G : H_C]$. Pero

$$[G : H_C] = \frac{o(G)}{o(H_C)} = \frac{p^n m}{p^k m'} = p^{n-k} \frac{m}{m'}.$$

Así p^{n-h+1} no divide a p^{n-k}, de donde $n - k < n - h + 1$, es decir $k \geq h$. Por tanto $o(H_C) \geq p^h$.

Por otra parte, como

$$H_C = \{g \in G : gC = C\},$$

fijado un $c_1 \in C$ se tiene que $gc_1 \in C$ para todo $g \in H_C$. Supongamos que

$$C = \{c_1, \ldots, c_{o(C)}\} \qquad \text{con} \qquad o(C) = p^h.$$

Se tiene que

$$gc_1 \in \{c_1, \ldots, c_{o(C)}\},$$

es decir $g = c_i c_1^{-1}$ para cierto c_i. Así, a lo sumo, hay tantos $g \in H_C$ como elementos tiene C, de donde

$$o(H_C) \leq \text{card}(C) = p^h.$$

Por tanto $o(H_C) = p^h$.

■

Como consecuencia del Primer Teorema de Sylow podemos obtener el Teorema de Cauchy.

Corolario 5.3.2 (Teorema de Cauchy) *Sea G un grupo finito. Si p es un divisor primo del orden de G, entonces G posee un elemento de orden p.*

Definición 5.3.3 *Sean G un grupo finito, p un número primo que divide al orden de G y H un subgrupo de G. Diremos que:*

1. *H es un p-subgrupo de G si H es un p-grupo.*

2. *H es un p-subgrupo de Sylow de G si el orden de H es p^h, siendo p^h la máxima potencia de p que divide al orden de G.*

Observación 5.3.4 *El Primer Teorema de Sylow nos asegura que en un grupo finito, siempre existe un p-subgrupo de Sylow para cada divisor primo del orden del grupo. Esto es un recíproco parcial del Teorema de Lagrange.*

Ejemplo 5.3.5 *Dado un grupo G tal que $o(G) = 2^3 5^2$, el Teorema 5.3.1 nos asegura que G tiene un 2-subgrupo de Sylow de orden 8 y un 5-subgrupo de Sylow de orden 25.*

Teorema 5.3.6 (Segundo Teorema de Sylow) *Sea G un grupo tal que $o(G) = p^n m$, con p primo y $\text{mcd}(p, m) = 1$. Sean H un p-subgrupo de G y S un p-subgrupos de Sylow de G. Entonces existe $g \in G$ tal que $g^{-1} H g \subseteq S$.*

DEMOSTRACIÓN. Consideremos el conjunto $G/\mathcal{R}^S = \{gS : g \in G\}$. La aplicación definida por

$$\begin{aligned} H \times G/\mathcal{R}^S &\longrightarrow G/\mathcal{R}^S \\ (h, gS) &\longmapsto hgS \end{aligned}$$

es una acción de H sobre $G/\mathcal{R}^S$. Como $o(G) = p^n m$ y $o(S) = p^n$ tenemos, por el Corolario 5.1.10,

$$m = \text{card}\left(G/\mathcal{R}^S\right) = \sum_{gS \in G/H} [H : H_{gS}].$$

Como H_{gS} es un subgrupo de H y $o(H) = p^h$, tenemos que $[H : H_{gS}]$ es un múltiplo de p.

Por otra parte, si no existiese ningún g tal que $[H : H_{gS}] = 1$, tendríamos que p divide a m y eso es contradictorio con el hecho de que $\text{mcd}(p, m) = 1$.

Así, existe $g \in G$ tal que $[H : H_{gS}] = 1$, es decir

$$H = H_{gS} = \{h \in H : hgS = gS\}.$$

Por tanto para todo $h \in H$ se tiene que $hgS = gS$, es decir $g^{-1}hgS = S$. Así $g^{-1}Hg \subseteq S$.

■

Como consecuencia tenemos que

Corolario 5.3.7 *Todos los p-subgrupos de Sylow de G son conjugados. En particular, si S es subgrupo normal de G y S es p-subgrupo de Sylow, entonces S es el único p-subgrupo de Sylow de G.*

Veamos que el recíproco de la segunda afirmación del Corolario 5.3.7 también es cierto.

Corolario 5.3.8 *Sea H el único p-subgrupo de Sylow de un grupo G, entonces H es normal en G.*

DEMOSTRACIÓN. Para todo $g \in G$, se tiene que gHg^{-1} es subgrupo de G y $o(gHg^{-1}) = o(H)$. Por tanto, gHg^{-1} es un p-subgrupo de Sylow. Pero al ser H el único p-subgrupo de Sylow de G, se tiene que $gHg^{-1} = H$. Así H es subgrupo normal en G.

■

Antes de demostrar el Tercer Teorema de Sylow daremos algunas definiciones y propiedades que se requieren en su demostración.

Definición 5.3.9 *Sea H un subgrupo del grupo G. Llamamos normalizador de H en G, y lo denotamos por $N_G(H)$, al siguiente conjunto*

$$N_G(H) = \left\{ g \in G : \ g^{-1}Hg = H \right\}.$$

Lema 5.3.10 *Sea G un grupo y H un subgrupo de G, entonces se verifica:*

1. *$N_G(H)$ es subgrupo de G.*
2. *H es subgrupo normal de $N_G(H)$.*
3. *$N_G(H)$ es el mayor subgrupo de G en el que H es normal.*

DEMOSTRACIÓN.

(1) (a) $N_G(H) \neq \emptyset$, ya que $1 \in N_G(H)$.

(b) $N_G(H) \subseteq G$ por definición.

(c) Para todo $x \in N_G(H)$, se tiene que $x^{-1}Hx = H$, así $H = xHx^{-1}$, es decir $H = (x^{-1})^{-1}Hx^{-1}$, por tanto $x^{-1} \in N_G(H)$.

(d) Sean $x, y \in N_G(H)$, entonces

$$x^{-1}Hx = H, \qquad y^{-1}Hy = H.$$

Por tanto,

$$(xy)^{-1}H(xy) = y^{-1}(x^{-1}Hx)y = y^{-1}Hy = H.$$

Así, $xy \in N_G(H)$.

(2) Por definición de $N_G(H)$ se tiene que para todo $g \in N_G(H)$ se verifica

$$g^{-1}Hg = H,$$

y de ahí, por la Proposición 1.6.3, se tiene que H es normal en $N_G(H)$.

(3) Sea K un subgrupo de G, tal que H sea normal en K. Entonces por la Proposición 1.6.3 se tiene que para todo $k \in K$ se verifica $kH = Hk$. Así $k^{-1}Hk = H$ y de ahí $k \in N_G(H)$.

■

Lema 5.3.11 *Si P es un p-subgrupo de Sylow del grupo finito G, entonces todo p-subgrupo de $N_G(P)$ está contenido en P.*

DEMOSTRACIÓN. Sea Q un p-subgrupo de $N_G(P)$. Veamos que $Q \subseteq P$. Tenemos que P y Q son subgrupos de $N_G(P)$. Por el Lema 5.3.10 se tiene que P normal en $N_G(P)$ y por el Corolario 5.3.7 es el único. Como $N_G(P)$ es subgrupo de G, entonces P es un p-subgrupo de Sylow de $N_G(P)$. Como Q es un p-subgrupo de $N_G(P)$, entonces por el Segundo Teorema de Sylow, aplicado a $N_G(P)$, existe $g \in N_G(P)$ tal que $g^{-1}Qg \subseteq P$. Por tanto,

$$Q \subseteq gPg^{-1} = P,$$

al ser P subgrupo normal en $N_G(P)$.

■

Teorema 5.3.12 (Tercer Teorema de Sylow) *Sea G un grupo tal que $o(G) = p^n m$, con p primo y $\mathrm{mcd}(p, m) = 1$. Sea P un p-subgrupo de Sylow, y sea n_p el número de p-subgrupos de Sylow de G. Entonces:*

1. $n_p = [G : N_G(P)]$.
2. *n_p divide a m y $n_p \equiv 1 (mód\ p)$,*

DEMOSTRACIÓN.

(1) Consideremos el conjunto

$$\mathcal{P} = \{Q : Q \text{ es } p\text{-subgrupo de Sylow de } G\}.$$

Definimos la aplicación

$$\begin{array}{rcl} G \times \mathcal{P} & \longrightarrow & \mathcal{P} \\ (g, Q) & \longmapsto & gQg^{-1}. \end{array}$$

Se tiene que $\mathcal{P}$ es un G-conjunto. Para esta acción se tiene que

$$H_P = \left\{g \in G : gPg^{-1} = P\right\} = N_G(P).$$

Por el Segundo Teorema de Sylow, se tiene

$$\mathcal{O}_P = \left\{gPg^{-1} : g \in G\right\} = \mathcal{P}.$$

Por tanto,

$$n_p = \mathrm{card}(\mathcal{P}) = \mathrm{card}\left(\mathcal{O}_P\right) = [G : H_P] = [G : N_G(P)],$$

lo que demuestra el apartado (1).

(2) Por el apartado (1) se tiene que

$$n_p = [G : N_G(P)] = \frac{p^n m}{o(N_G(P))} = \frac{p^n m}{p^n m'} = \frac{m}{m'} \in \mathbb{Z}$$

y $\dfrac{m}{m'}$ divide a m.

Consideremos el conjunto $G/N_G(P)$, y definamos la acción

$$\begin{array}{rcl} P \times G/N_G(P) & \longrightarrow & G/N_G(P) \\ (x, gN_G(P)) & \longmapsto & xgN_G(P). \end{array}$$

Por el Corolario 5.1.10 se tiene

$$[G : N_G(P)] = \sum_{gN_G(P) \in G/N_G(P)} [P : H_{gN_G(P)}].$$

Como $o(P) = p^n$ se tiene que $[P : H_{gN_G(P)}]$ es 1 ó un múltiplo de p.

Vamos a contar cuántos elementos $gN_G(P)$ existen cuya órbita sea un conjunto unitario, es decir cuántos elementos hay tales que

$$\{gN_G(P)\} = \mathcal{O}_{gN_G(P)},$$

donde recordamos que

$$\mathcal{O}_{gN_G(P)} = \{xgN_G(P) : x \in P\}.$$

Así, estamos contando los elementos $gN_G(P)$ tales que

$$xgN_G(P) = gN_G(P) \qquad \text{para todo} \qquad x \in P,$$

o lo que es equivalente, a $g^{-1}xg \in N_G(P)$ para todo $x \in P$. Por tanto $g^{-1}Pg \subseteq N_G(P)$.

Como $o(g^{-1}Pg) = o(P)$, se tiene que $g^{-1}Pg$ y P son p-subgrupos de Sylow de $N_G(P)$. Entonces por el Segundo Teorema de Sylow, existe $h \in N_G(P)$ tal que $h^{-1}Ph = g^{-1}Pg$, es decir $gh^{-1}Phg^{-1} = P$. Por tanto $gh^{-1} \in N_G(P)$, de donde $g \in N_G(P)$.

Así podemos afirmar que la órbita $\mathcal{O}_{N_G(P)}$ es la única órbita que tiene un único elemento, de donde $n_p \equiv 1 \pmod{p}$.

■

Como consecuencia de los Corolarios 5.3.7 y 5.3.8 tenemos la siguiente caracterización de los subgrupos normales.

Corolario 5.3.13 *Sea G un grupo finito y p un número primo tal que p divide a $o(G)$. Si H es un p-subgrupo de Sylow de G, entonces:*

1. *H es un subgrupo normal de $G \iff n_p = 1$.*
2. *Si G es un grupo abeliano, entonces $n_p = 1$.*

Ejemplo 5.3.14 *Vamos a calcular los p-subgrupos de Sylow de un grupo G de orden 15.*

Como $15 = 3 \cdot 5$, por el Primer Teorema de Sylow sabemos que existe un 3-subgrupo de Sylow P_3 tal que $o(P_3) = 3$ y un 5-subgrupo de Sylow P_5 tal que $o(P_5) = 5$.

Vamos a ver cuántos hay de cada clase.

El número de 3-subgrupos de Sylow, n_3, por el Tercer Teorema de Sylow, debe de verificar:

$$n_3 \text{ divide a } 5.$$

De donde $n_3 = \{1, 5\}$. Pero como

$$n_3 \equiv 1 \,(\text{mód } 3),$$

se tiene que $n_3 = 1$. Razonando de la misma manera para n_5 se tiene que $n_5 = 1$. Por tanto podemos afirmar que G contiene un único 3-subgrupo de Sylow, P_3 y un único 5-subgrupo de Sylow, P_5. Por el Corolario 5.3.13, P_3 y P_5 son subgrupos normales.

Como $P_3 \cap P_5 = \{1\}$, al ser subgrupos normales, se verifica que P_3P_5 es un subgrupo de G de orden 15. Entonces se puede afirmar que $G = P_3P_5$, y por la Proposición 2.4.9, se tiene

$$G = P_3P_5 \cong P_3 \times P_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}.$$

Teorema 5.3.15 *Sea G un grupo finito tal que $o(G) = p_1^{n_1} \cdots p_r^{n_r}$. Son equivalentes:*

1. *Los p-subgrupos de Sylow de G son normales.*
2. *$G \cong P_1 \times \cdots \times P_r$, siendo P_i un p_i-subgrupo de Sylow de G.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2): Definimos la aplicación

$$\begin{aligned} \varphi : P_1 \times P_2 \times \cdots \times P_r &\longrightarrow G \\ (x_1, x_2, \ldots, x_r) &\longmapsto x_1x_2 \cdots x_r. \end{aligned}$$

(a) Veamos que φ es homomorfismo de grupos. Como

$$\varphi[(x_1, x_2, \ldots, x_r)(y_1, y_2, \ldots, y_r)] = \varphi(x_1y_1, \ldots, x_ry_r) = x_1y_1 \cdots x_ry_r,$$

para demostrar que φ es un homomorfismo de grupos bastará demostrar que dados $x \in P_i$, $y \in P_j$ con $i \neq j$ se tiene que $xy = yx$.
Se verifica que

$$xyx^{-1}y^{-1} \in P_j \text{ ya que } xP_jx^{-1} = P_j$$

y

$$xyx^{-1}y^{-1} \in P_i \text{ ya que } yP_iy^{-1} = P_i.$$

Como $P_i \cap P_j = \{1\}$ ya que $\text{mcd}(p_i, p_j) = 1$, se tiene

$$xyx^{-1}y^{-1} = 1$$

y de ahí que $xy = yx$. Así φ es un homomorfismo de grupos.

(b) Veamos que φ es sobreyectiva. Como $o(G) = p_1^{n_1} \cdots p_r^{n_r}$, definimos

$$q_i = \frac{o(G)}{p_i^{n_i}}.$$

Como $\text{mcd}(p_1, \ldots, p_r) = 1$ se tiene que $\text{mcd}(q_1, \ldots, q_r) = 1$, y por tanto existen $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ tales que

$$\alpha_1q_1 + \cdots + \alpha_rq_r = 1.$$

Así dado $x \in G$, se tiene que

$$x = x^{\alpha_1q_1 + \cdots + \alpha_rq_r} = x^{\alpha_1q_1} \cdots x^{\alpha_rq_r}.$$

Denotamos $x_i = x^{\alpha_iq_i}$, $i = 1, \ldots, r$. Se tiene que

$$x_i^{p_i{}^{n_i}} = (x^{\alpha_iq_i})^{p_i{}^{n_i}} = x^{\alpha_i{}^{o(G)}} = \left(x^{o(G)}\right)^{\alpha_i} = 1.$$

Por tanto se tiene que el orden de x_i divide a $p_i{}^{n_i}$. Así tenemos que el orden del subgrupo $\langle x_i \rangle$, divide al orden del p_i-subgrupo de Sylow P_i. Pero por hipótesis P_i es un subgrupo normal en G, entonces se tiene que $N_G(P_i) = G$. Así, aplicando el Lema 5.3.11, se tiene que $\langle x_i \rangle \subseteq P_i$, de donde $x_i \in P_i$ y de ahí podemos afirmar que φ es sobreyectiva.

(c) φ es inyectiva. Se tiene que

$$o(G) = o(P_1 \times \cdots \times P_r).$$

Por otro lado se tiene que

$$P_1 \times \cdots \times P_r / \ker(\varphi) \cong G.$$

De donde $o(\ker(\varphi)) = 1$. Así $\ker(\varphi) = \{1\}$ y por tanto φ es inyectiva.

(2) $\Longrightarrow$ (1): Sin pérdida de generalidad podemos suponer que $G = P_1 \times \cdots \times P_r$. Como

$$\begin{cases} P_1 \times \{1\} \times \cdots \times \{1\} \cong P_1 \\ \vdots \\ \{1\} \times \{1\} \times \cdots \times P_r \cong P_r \end{cases}$$

y $o(P_i) = p_i^{n_i}$. Es claro que todo P_i es subgrupo normal de G.

■

5.4. Aplicaciones

Como aplicación de los teoremas de Sylow, podemos presentar algunos grupos para los que es cierto el recíproco del Teorema de Lagrange.

Proposición 5.4.1 *El recíproco del Teorema de Lagrange es cierto para todo p-grupo G.*

DEMOSTRACIÓN. Por hipótesis, $o(G) = p^m$, siendo p primo y $m \geq 1$. Por el Primer Teorema de Sylow, para todo $0 \leq h \leq m$ existe un subgrupo H de G tal que $o(H) = p^h$.

■

Proposición 5.4.2 *El recíproco del Teorema de Lagrange es cierto en los grupos de orden 20, y en general en los grupos de orden pq, siendo p y q números primos entre sí.*

DEMOSTRACIÓN. Sea G un grupo de orden 20. Se tiene que $20 = 2^2 \cdot 5$. Los divisores de 20 son $\{1, 2, 4, 5, 10, 20\}$.

Los subgrupos $\{1\}$ y G tienen el orden 1 y 20 respectivamente. Por el Primer Teorema de Sylow, tenemos que G posee subgrupos de órdenes 2, 4 y 5. Sólo nos falta encontrar el subgrupo de orden 10.

Por el Tercer Teorema de Sylow, el número n_5 de 5-subgrupos de Sylow de G verifica:

- n_5 divide a 4.
- $n_5 - 1$ es múltiplo de 5.

Por lo tanto $n_5 = 1$. Denotemos por H el único subgrupo de orden 5. Por el Corolario 5.3.13 tenemos que H es subgrupo normal de G.

Entonces si K es un subgrupo de orden 2 de G, por la Proposición 1.2.21, se tiene que HK es un subgrupo de G. Como $o(H \cap K) = \{1\}$ ya que $\text{mcd}(2,5) = 1$ se tiene que

$$o(HK) = o(H)o(K) = 10,$$

por la Proposición 1.3.7 ó por la Proposición 2.4.9.

■

5.5. Ejercicios

1. Sean p es un número primo, m, n enteros positivos y

$$N = \begin{pmatrix} p^n m \\ p^n \end{pmatrix}.$$

Demostrad que las máximas potencias de p que dividen a N y a m coinciden.

2. Demostrad que para todo subgrupo H de un grupo G se tiene que:

   a) $C_G(H) \triangleleft N_G(H)$, donde $C_G(H) = \{a \in G : ah = ha, \forall h \in H\}$

   b) El subgrupo cociente $N_G(H)/C_G(H)$ es isomorfo a un subgrupo de $Aut(H)$.

3. Sea G un grupo que opera sobre un conjunto X. Se supone que $o(G) = 35$, $card(X) = 19$ y que X no tiene órbitas con un solo elemento. Calculad el número de órbitas y el cardinal de cada órbita.

4. Contestad a las siguientes cuestiones:

   a) ¿Qué orden tiene un 3-subgrupo de Sylow de un grupo de orden 54?.

   b) Un grupo de orden 24, ¿Cuántos 2-subgrupos de Sylow debe tener?

   c) Un grupo de orden 255 ¿Cuántos 3-subgrupos de Sylow puede tener? ¿Y 5-subgrupos de Sylow?

5. Probad que no existen grupos simples de orden 200 ni de orden 1000.

6. Demostrad que todo grupo de orden 1225 es abeliano.

7. Demostrad que si G es un grupo de orden 12, bien posee un 2-subgrupo de Sylow que es normal, o bien posee un 3-subgrupo de Sylow que es normal.

8. Demostrad que todo grupo de orden 30 posee un único 3-subgrupo de Sylow y un único 5-subgrupo de Sylow. En particular, los grupos de orden 30 no son simples.

9. Sean p y q números primos tales que $p < q$ y $q - 1$ no es múltiplo de p. Demostrad que todo grupo de orden pq es isomorfo a $Z/pq\mathbb{Z}$.

10. Demostrad que un grupo no abeliano G de orden p^3, donde p es un número primo, tiene un centro de orden p.

11. Sea G un grupo y $o(G) = p^2q$, donde p y q son números primos distintos y tales que $p^2 - 1$ no es múltiplo de q y $q - 1$ no es múltiplo de p. Demostrad que G es abeliano y de ahí que G no es simple.

12. Demostrad que un grupo finito G es un p-grupo si, y sólo si, el orden de todo elemento de G es una potencia de p.

13. Demostrad que todo grupo $(G, *)$ de orden 8 posee subgrupos de órdenes 2 y 4.

14. Sea p un número primo mayor que 2 y G un grupo de orden $2p$. Demostrad que entonces G posee subgrupos de órdenes 2 y p, y que de orden p sólo hay uno.

15. Demostrad que si G es un grupo finito de orden $n < 12$, entonces para cada divisor d de n existe un subgrupo de G de orden d.

Capítulo 6

Series de grupos

El estudio de las propiedades de un grupo a través de sus series normales hunde sus raíces en los orígenes mismos del estudio de los grupos. Abel, en sus trabajos sobre resolubilidad de ecuaciones polinomiales, estudia esta propiedad a través de la "resolubilidad" de un grupo asociado a cada polinomio. Esta "resolubilidad" depende de la existencia de una cierta serie normal. En este capítulo nos centraremos en cuatro tipos de grupos, caracterizados por series normales, y estudiaremos las propiedades inducidas por la existencia de dichas series.

6.1. Series normales

Definición 6.1.1 *Una serie normal de un grupo G es una sucesión finita de subgrupos de G*

$$S : \{1_G\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

de modo que para cada $1 \leq i \leq n$, G_{i-1} es subgrupo normal de G_i.

Los cocientes G_i/G_{i-1} se llaman factores de la serie S y el número n se llama longitud de S, que denotaremos $\log(S) = n$.

Ejemplo 6.1.2 *Dos series normales de $\mathbb{Z}$*

$$S : \{0\} \subset 8\mathbb{Z} \subset 4\mathbb{Z} \subset \mathbb{Z}$$

$$T : \{0\} \subset 9\mathbb{Z} \subset \mathbb{Z}.$$

Definición 6.1.3 *Dadas dos series S y T de un grupo G, diremos que T es un refinamiento de S si cada término de S lo es de T. Si $S \neq T$, decimos que es un refinamiento propio.*

Ejemplo 6.1.4 *La serie*

$$T : \{0\} \subset 72\mathbb{Z} \subset 24\mathbb{Z} \subset 8\mathbb{Z} \subset 4\mathbb{Z} \subset \mathbb{Z}$$

es un refinamiento de la serie

$$S : \{0\} \subset 72\mathbb{Z} \subset 8\mathbb{Z} \subset \mathbb{Z},$$

puesto que se han insertado dos nuevos términos, $4\mathbb{Z}$ *y* $24\mathbb{Z}$.

Ejemplo 6.1.5 *Consideremos el grupo* S_4 *de las permutaciones de* 4 *elementos, y sea* A_4 *el subgrupo alternado de* S_4. *Como se verifica que* $[S_4 : A_4] = 2$, *se tiene que* A_4 *es un subgrupo normal de* S_4. *Por tanto,*

$$S : \{Id\} \subset A_4 \subset S_4$$

es una serie normal de S_4 *de longitud* 2.

Pero como A_4 *tiene un subgrupo normal* V *(ver Ejemplos 5.1.8(2)) de orden* 4, *la serie*

$$T : \{Id\} \subset V \subset A_4 \subset S_4$$

es un refinamiento propio de S_4.

Definición 6.1.6 *Una serie* S *de un grupo* G *es una serie de composición si no admite refinamientos propios.*

Para decidir si una serie es de composición utilizaremos el siguiente criterio, cuya demostración dejaremos como ejercicio para el lector.

Proposición 6.1.7 *Una serie*

$$S : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

es serie de composición si y sólo si los factores G_i/G_{i-1} *son grupos simples.*

Ejemplo 6.1.8 *La serie del Ejemplo 6.1.5*

$$S : \{Id\} \subset V \subset A_4 \subset S_4$$

no es de composición ya que $V/\{1\} = V$, *y* V *no es simple ya que tiene orden* 4.

Lema 6.1.9 *Sea* G *un grupo, y sea* H *un subgrupo normal de* G. *Entonces* G *admite una serie de composición si y sólo si* H *y* G/H *la admiten.*

DEMOSTRACIÓN. $\Longrightarrow$ Sea

$$S : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

una serie de composición de G. Tomemos los subgrupos de H, $H_i = H \cap G_i$ y observemos que

- $H_{i-1} \subset H_i$ para $1 \leq i \leq n$.
- H_{i-1} es subgrupo normal de H_i. Vamos a verlo:

  Dados $a, b \in H_i$, tales que $ab \in H_{i-1} = H \cap G_{i-1}$, tenemos que $ab \in G_{i-1}$. Como $a.b \in H_i$, se verifica que $a, b \in G_i$, y al ser G_{i-1} subgrupo normal de G_i, tenemos que $ba \in G_{i-1}$. Por otro lado $a, b \in H$, y al ser H subgrupo, tenemos que $ba \in H$, de donde

  $$ba \in G_{i-1} \cap H = H_{i-1}.$$

  Por tanto H_{i-1} es normal en H_i.

- Observemos que, al verificarse

  $$H_{i-1} = H \cap G_{i-1} = H \cap (G_{i-1} \cap G_i) = (H \cap G_i) \cap G_{i-1} = H_i \cap G_{i-1},$$

  por el Tercer Teorema de Isomorfía tenemos que

  $$H_i/H_{i-1} = H_i/(H_i \cap G_{i-1}) \cong (G_{i-1}H_i)/G_{i-1}.$$

  Pero $(G_{i-1}H_i)/G_{i-1}$ es un subgrupo normal del grupo G_i/G_{i-1}. Por tanto, si G_i/G_{i-1} es simple entonces H_i/H_{i-1} también es simple o $H_i = H_{i-1}$.

Así, eliminando los términos superfluos, podemos afirmar que la serie

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_n = H$$

es una serie de composición para H.

Consideremos ahora el grupo G/H, y observemos que, al igual que antes, se verifica:

- $G_i \cap H$ es subgrupo normal de G_i.
- $G_{i-1}/(G_{i-1} \cap H)$ es isomorfo a un subgrupo normal de $G_i/(G_i \cap H)$ para cada $1 \leq i \leq n$.

- $(G_i/G_i \cap H) \,/\, (G_{i-1}/(G_{i-1} \cap H))$ es simple. Vamos a verlo:
  Por el Segundo y Tercer Teorema de Isomorfía, se tiene que:

$$\frac{G_i/(G_i \cap H)}{G_{i-1}/(G_{i-1} \cap H)} \cong \frac{G_iH/H}{G_{i-1}H/H} \cong \frac{G_iH}{G_{i-1}H}.$$

  Pero $\dfrac{G_iH}{G_{i-1}H}$ es isomorfo a un subgrupo normal de $\dfrac{G_i}{G_{i-1}}$. Por tanto podemos afirmar que:

$$\frac{G_i/(G_i \cap H)}{G_{i-1}/(G_{i-1} \cap H)} \text{ es isomorfo a un subgrupo normal de } \frac{G_i}{G_{i-1}}.$$

  Así, $\dfrac{G_i/(G_i \cap H)}{G_{i-1}/(G_{i-1} \cap H)}$ es simple al ser simple el grupo $\dfrac{G_i}{G_{i-1}}$.

Eliminando términos superfluos, concluimos que la serie

$$\{1\} = \frac{G_0}{G_0 \cap H} \subset \frac{G_1}{G_1 \cap H} \subset \cdots \subset \frac{G_n}{G_n \cap H} = G/H,$$

es una serie de composición de G/H.

$\Longleftarrow$ Sean

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_k = H$$

y

$$\{1H\} = N_0 \subset N_1 \subset \cdots \subset N_l = G/H,$$

dos series de composición de H y G/H respectivamente. Entonces existen $G_0 = H, G_1, \cdots, G_l$ subgrupos de G que contienen a H y tales que $G_i/H = N_i$ para cada $1 \leq i \leq l$.

Para cada $1 \leq i \leq l$ se verifica que:

- $G_{i-1} \subset Gi$ ya que $N_{i-1} \subset N_i$.
- G_{i-1} es subgrupo normal de G_i ya que N_{i-1} es subgrupo normal de N_i.
- G_{i-1}/G_i es simple, ya que por el Segundo Teorema de Isomorfía se tiene que

$$G_i/G_{i-1} \cong \frac{G_i/H}{G_{i-1}/H} \cong N_i/N_{i-1}.$$

Por tanto la serie

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_k = H = G_0 \subset G_1 \subset \cdots \subset G_l = G,$$

es una serie de composición de G.

■

6.2. Teorema de Jordan-Hölder

En esta sección caracterizaremos la existencia de series de composición, así como la equivalencia de las mismas.

En general un grupo puede admitir más de una serie de composición. Por ejemplo, si $G = \mathbb{Z}/12\mathbb{Z}$, consideramos

$$G_1 = 6\mathbb{Z}/12\mathbb{Z}, \qquad G_2 = 3\mathbb{Z}/12\mathbb{Z},$$

y

$$H_1 = 4\mathbb{Z}/12\mathbb{Z}, \qquad H_2 = 2\mathbb{Z}/12\mathbb{Z}.$$

Las series

$$S : \{1\} = G_0 \subset G_1 \subset G_2 \subset G_3 = G,$$

$$T : \{1\} = H_0 \subset H_1 \subset H_2 \subset H_3 = G,$$

son de composición.

Con objeto de probar que los grupos que admiten una serie de composición tienen todas sus series de composición unívocamente determinadas, procedemos a introducir una noción de equivalencia para comparar series.

Definición 6.2.1 *Decimos que dos series*

$$S : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

$$T : \{1\} = H_0 \subset H_1 \subset \cdots \subset H_m = G,$$

de un grupo G son equivalentes si $n = m$ y existe una permutación $\sigma \in S_n$ tal que

$$G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i-1)} \quad \text{para cada} \quad 1 \leq i \leq n.$$

Para probar el Lema de la mariposa, resultado técnico esencial para nuestro objetivo, vamos a utilizar el siguiente resultado, cuya demostración es un cálculo simple.

Lema 6.2.2 *Sean A, B y C tres subgrupos de un grupo G, tales que $B \subset A$. Entonces*

$$A \cap BC = B\,(A \cap C)\,.$$

Lema 6.2.3 (Lema de la mariposa o de Zassenhaus) *Sean G un grupo y H_1, H_2, N_1, N_2 subgrupos de G, donde N_1 es subgrupo normal de H_1 y N_2 es subgrupo normal de H_2. Entonces*

1. *$N_1(H_1 \cap H_2)$ es subgrupo de H_1 y $N_2(H_1 \cap H_2)$ es subgrupo de H_2.*

2. $N_1(H_1 \cap N_2)$ *es subgrupo normal de* $N_1(H_1 \cap H_2)$ *y* $N_2(N_1 \cap H_2)$ *es subgrupo normal de* $N_2(H_1 \cap H_2)$.

3. $(H_1 \cap N_2)(H_2 \cap N_1)$ *es subgrupo normal de* $H_1 \cap H_2$.

4. $\dfrac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \cong \dfrac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)} \cong \dfrac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)}$.

DEMOSTRACIÓN.

(1) Se tiene que H_1 y $H_1 \cap H_2$ son subgrupos de H_1 donde $N_1 \lhd H_1$ entonces por el apartado (3) del Tercer Teorema de Isomorfia, se tiene que

$$N_1 (H_1 \cap H_2) \text{ es subgrupo de } H_1.$$

De forma análoga podemos afirmar que

$$N_2 (H_1 \cap H_2) \text{ es subgrupo de } H_2.$$

(2) Se tiene que $H_1 \cap H_2$ y N_2 son subgrupos de H_2 con N_2 normal en H_2. Entonces por el apartado (1) del Tercer Teorema de Isomorfía, se tiene que

$$H_1 \cap H_2 \cap N_2 \text{ es subgrupo normal de } H_1 \cap H_2.$$

Por tanto

$$H_1 \cap N_2 \text{ es subgrupo normal de } H_1 \cap H_2.$$

Por otro lado tenemos que N_1 es subgrupo normal de H_1, $H_1 \cap N_2$ y $H_1 \cap H_2$ son subgrupos de H_1 tales que $H_1 \cap N_2$ es normal en $H_1 \cap H_2$. Entonces por el Lema 1.6.7 se tiene

$$N_1 (H_1 \cap N_2) \text{ es subgrupo normal de } N_1 (H_1 \cap H_2).$$

De forma análoga se demuestra la segunda afirmación.

(3) Al verificarse que $H_1 \cap N_2 \subseteq H_1 \cap H_2$ y $N_1 \cap H_2 \subseteq H_1 \cap H_2$, se tiene que

$$(H_1 \cap N_2)(N_1 \cap H_2) \subseteq (H_1 \cap H_2).$$

En el apartado anterior hemos demostrado, bajo las condiciones de las hipótesis, que $H_1 \cap N_2$ es subgrupo normal de $H_1 \cap H_2$. Por tanto podemos afirmar que

$$(H_1 \cap N_2)(N_1 \cap H_2) \text{ es subgrupo de } H_1 \cap H_2.$$

Veamos que es subgrupo normal. Para ello demostraremos que dado cualquier $a \in H_1 \cap H_2$, se tiene

$$a(H_1 \cap N_2)(N_1 \cap H_2) = (H_1 \cap N_2)(N_1 \cap H_2)a.$$

Sea $x \in a(H_1 \cap N_2)(N_1 \cap H_2)$, entonces

$$x = auv, \qquad \text{con} \qquad u \in H_1 \cap N_2, \qquad v \in N_1 \cap H_2. \tag{i}$$

Como $au \in aN_2$, donde $a \in H_2$ y $N_2 \lhd H_2$, entonces

$$au = n_2 a \qquad \text{donde} \qquad n_2 \in N_2. \tag{ii}$$

Es más, $n_2 = aua^{-1} \in H_1$, ya que $a, u \in H_1$. Así, sustituyendo (ii) en (i),

$$x = auv = n_2 av \qquad \text{con} \qquad n_2 \in H_1 \cap N_2.$$

Como $av \in aN_1$, donde $a \in H_1$, $v \in N_1$ y $N_1 \lhd H_1$, entonces

$$av = n_1 a \qquad \text{donde} \qquad n_1 \in N_1 \tag{iii}$$

y $n_1 = ava^{-1} \in H_2$ ya que $a, v \in H_2$. Luego, sustituyendo (iii) en (ii),

$$x = n_2 n_1 a \qquad \text{con} \qquad n_2 \in H_1 \cap N_2, \qquad n_1 \in N_1 \cap H_2,$$

es decir $x \in (H_1 \cap N_2)(N_1 \cap H_2)a$. Por tanto,

$$a(H_1 \cap N_2)(N_1 \cap H_2) \subseteq (H_1 \cap N_2)(N_1 \cap H_2)a.$$

De forma análoga obtenemos la otra inclusión y de ahí el resultado.

(4) Si denotamos

$$H = H_1 \cap H_2, \qquad N = N_1(H_1 \cap N_2), \qquad G' = N_1(H_1 \cap H_2),$$

se tiene que H y N son subgrupos de G' donde por el apartado (2), se tiene que $N \lhd G'$. Entonces por el Tercer Teorema de Isomorfía se tiene que

$$\frac{N_1(H_1 \cap N_2)(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} = \frac{NH}{N} = \frac{HN}{N} \cong$$
$$\cong \frac{H}{H \cap N} = \frac{H_1 \cap H_2}{H_1 \cap H_2 \cap N_1(H_1 \cap N_2)}.$$

Para finalizar la demostración, vamos a usar dos veces el Lema 6.2.2. En el primer caso, consideremos los subgrupos

$$A = H_1, \qquad B = H_1 \cap N_2, \qquad C = H_2.$$

Al verificarse que $B \subset A$, se tiene que

$$H_1 \cap (H_1 \cap N_2) H_2 = (H_1 \cap N_2)(H_1 \cap H_2).$$

Pero $H_1 \cap N_2 \subseteq N_2 \subseteq H_2$, de donde $(H_1 \cap N_2) H_2 = H_2$, y así

$$H_1 \cap H_2 = (H_1 \cap N_2)(H_1 \cap H_2).$$

Consecuentemente

$$N_1 (H_1 \cap H_2) = N_1 (H_1 \cap N_2)(H_1 \cap H_2).$$

Por tanto

$$\frac{N_1 (H_1 \cap H_2)}{N_1 (H_1 \cap N_2)} \cong \frac{H_1 \cap H_2}{H_1 \cap H_2 \cap N_1 (H_1 \cap N_2)}.$$

Aplicando de nuevo el Lema 6.2.2 a los subgrupos

$$A = H_1 \cap H_2, \qquad B = H_1 \cap N_2, \qquad C = N_1,$$

obtenemos

$$H_1 \cap H_2 \cap (H_1 \cap N_2) N_1 = A \cap BC =$$

$$= B(A \cap C) = (H_1 \cap N_2)(H_1 \cap H_2 \cap N_1) =$$

$$= (H_1 \cap N_2)(N_1 \cap H_2),$$

ya que $N_1 \subseteq H_1$.

Luego

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \cong \frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)}.$$

De forma análoga se demuestra

$$\frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)} \cong \frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)},$$

y de ahí se obtiene el resultado.

■

Proposición 6.2.4 (Teorema de Schreier) *Dos series cualesquiera de un grupo G admiten refinamientos equivalentes.*

DEMOSTRACIÓN. Consideremos las series del grupo G,

$$S : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

$$T : \{1\} = H_0 \subset H_1 \subset \cdots \subset H_m = G.$$

Fijados $1 \leq i \leq n$, $1 \leq j \leq m$, tenemos $G_{i-1} \lhd G_i$ y $H_{j-1} \lhd H_j$.

Entonces, por el apartado (2) del Lema de la Mariposa, se tiene

$$G_{i-1}\left(G_i \cap H_{j-1}\right) \lhd G_{i-1}\left(G_i \cap H_j\right),$$

$$H_{j-1}\left(G_{i-1} \cap H_j\right) \lhd H_{j-1}\left(G_i \cap H_j\right),$$

y, por el apartado (4) del Lema de la Mariposa, se tiene

$$\frac{G_{i-1}\left(G_i \cap H_j\right)}{G_{i-1}\left(G_i \cap H_{j-1}\right)} \cong \frac{H_{j-1}\left(G_i \cap H_j\right)}{H_{j-1}\left(G_{i-1} \cap H_j\right)}. \tag{iv}$$

Además, como

$$G_0 = \{1\} = H_0. \qquad G_n = G = H_m, \qquad G_{i-1} \subset G_i \qquad \text{y} \qquad H_{j-1} \subset H_j,$$

se tiene

$$\begin{aligned} G_{i-1} &= G_{i-1}H_0 = G_{i-1}(G_i \cap H_0), \\ G_{i-1}\left(G_i \cap H_m\right) &= G_{i-1}G_i = G_i, \\ H_{j-1} &= H_{j-1}G_0 = H_{j-1}(H_j \cap G_0), \\ H_{j-1}\left(G_n \cap H_j\right) &= H_{j-1}H_j = H_j. \end{aligned}$$

Por tanto, podemos insertar en S y T estos subgrupos y construir un refinamiento de S,

$$S' : \{1\} = G_0 = G_0\left(G_1 \cap H_0\right) \subset G_0\left(G_1 \cap H_1\right) \subset \cdots \subset G_0\left(G_1 \cap H_m\right) = G_1 \subset$$

$$\subset \cdots \subset G_{i-1} = G_{i-1}(G_i \cap H_0) \subset G_{i-1}(G_i \cap H_1) \subset \cdots \subset$$

$$\subset G_{i-1}(G_i \cap H_m) = G_i \subset \cdots \subset G_n = G,$$

así como un refinamiento de T,

$$T' : \{1\} = H_0 = H_0\left(G_0 \cap H_1\right) \subset H_0\left(G_1 \cap H_1\right) \subset \cdots \subset H_0\left(G_n \cap H_1\right) = H_1 \subset$$

$$\subset \cdots \subset H_{j-1} = H_{j-1}(G_0 \cap H_j) \subset H_{j-1}(G_1 \cap H_j) \subset \cdots \subset$$

$$\subset H_{j-1}(G_n \cap H_j) = H_j \subset \cdots \subset H_m = G.$$

El número de eslabones en S' es $n(m-1)+n+1 = mn+1$, y el de T' es $m(n-1)+m+1 = mn+1$, luego coinciden.

Algunos eslabones en cada refinamiento pueden ser iguales, pero si hay r parejas de miembros consecutivos en S' iguales, hay r cocientes iguales a $\{1\}$ y por el isomorfismo (iv) hay también r cocientes iguales a $\{1\}$ en T' y por lo tanto el número de parejas de miembros consecutivos iguales en T' es también r. Si llamamos S'' a la serie obtenida a partir de S' eliminando los términos repetidos y T'' a la obtenida a partir de T' por el mismo procedimiento, hemos probado que

$$\text{long}(S'') = mn + 1 - r = \text{long}(T'').$$

Estos son los refinamientos buscados, pues al ser

$$G_{i-1}(G_i \cap H_m) = G_i, \qquad H_{j-1}(G_n \cap H_j) = H_j.$$

S'' refina a S y T'' refina a T, mientras que los factores de S'' son isomorfos a los de T'' por el isomorfismo (iv).

■

Corolario 6.2.5 (Teorema de Jordan-Hölder) *Dos series de composición de un grupo G son equivalentes.*

DEMOSTRACIÓN. Sean S y T series de composición de G. Por el Teorema de Schreier existen refinamientos equivalentes S' y T' de S y T respectivamente. Como S y T son series de composición, se tiene que S' y T' son equivalentes a S y T respectivamente. Por lo tanto, S y T son equivalentes.

■

6.3. Grupos Policíclicos

En esta sección estudiamos los grupos que poseen series asociadas a grupos cíclicos. En este caso, la existencia de dichas series establecen la propiedad de generación finita sobre el grupo.

Definición 6.3.1 *Decimos que una serie es cíclica si sus factores son grupos cíclicos. Decimos que el grupo G es policíclico si admite una serie cíclica.*

Lema 6.3.2 *Todo refinamiento de una serie cíclica es una serie cíclica.*

DEMOSTRACIÓN. Consideremos

$$S : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

una serie cíclica. Sea $1 \leq i \leq n$ y

$$G_{i-1} = H_0 \subset H_1 \subset \cdots \subset H_k = G_i$$

el trozo de un refinamiento S' de S, comprendido entre G_{i-1} y G_i. Todo se reduce a probar que los cocientes H_j/H_{j-1}, $1 \leq j \leq k$, son cíclicos.

Como $G_{i-1} \lhd G_i$, se tiene que $G_{i-1} \lhd H_j$ y $G_{i-1} \lhd H_{j-1}$. Entonces por el Segundo Teorema de Isomorfía

$$\frac{H_j}{H_{j-1}} \cong \frac{H_j/G_{i-1}}{H_{j-1}/G_{i-1}},$$

luego basta probar que H_j/G_{i-1} es cíclico. Como H_j/G_{i-1} es subgrupo del grupo cíclico G_i/G_{i-1}, entonces por el Teorema 1.4.7 se tiene el resultado.

■

Proposición 6.3.3 *Sean G un grupo y H un subgrupo normal de G. Entonces las siguientes afirmaciones son equivalentes:*

1. *G es policíclico.*
2. *H y G/H son policíclicos.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2): Si G es un grupo policíclico, entonces existirá

$$S : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

una serie cíclica de G. Como H es subgrupo de G podemos considerar los subgrupos H_i de G dados por

$$H_i = H \cap G_i.$$

Sea la sucesión

$$T : \{1\} = H_0 \subset H_1 \subset \cdots \subset H_{m-1} \subset H_m = H$$

donde $m \leq n$.

Análogamente a la demostración del Lema 6.1.9, se verifica que:

- H_i es subgrupo de H.
- H_{i-1} es subgrupo normal de H_i.
- Cada factor H_i/H_{i-1} es isomorfo a un subgrupo cíclico del grupo cíclico G_i/G_{i-1}. Así, por el Teorema 1.4.7 y la Proposición 2.2.14(2), es cíclico y de ahí que los factores H_i/H_{i-1} sean cíclicos.

Para la segunda parte consideremos los subgrupos $\widetilde{H}_i = G_i H$. Veamos que $\widetilde{H}_{i-1}$ es un subgrupo normal de $\widetilde{H}_i$.

Se verifica que:

- $\widetilde{H}_{i-1} = G_{i-1}H \subset G_i H = \widetilde{H}_i$.
- $G_{i-1}H$ es subgrupo normal de $G_i H$. Vamos a verlo:
  Si $x \in HG_{i-1}$, se escribirá $x = hg$ con $h \in H, g \in G_{i-1}$. Así $x \in Hg = gH \in G_{i-1}H$, ya que H es un subgrupo normal de G.
  Esto prueba la inclusión $HG_{i-1} \subseteq G_{i-1}H$. Simétricamente se obtiene la otra inclusión. Esto prueba que $G_{i-1}H$ es subgrupo de $G_i H$.

Para probar la normalidad usaremos la condición (1) de la Proposición 1.6.3. Tendremos que ver que para todo $a \in HG_i$ se tiene

$$a\,(HG_{i-1}) = (HG_{i-1})\,a.$$

Como $a \in HG_i$, se escribirá

$$a = hg, \quad h \in H, \quad g \in G_i. \tag{iv}$$

Como $HG_{i-1} = G_{i-1}H$, si $x \in a\,(HG_{i-1})$ se tiene

$$x = ag_1 h, \quad g_1 \in G_{i-1}, \quad h \in H.$$

Como $(ag_1)H = H(ag_1)$, por ser $H \lhd G$, si $x \in (ag_1)H$, sustituyendo en (iv), tendremos que

$$x = h_1 a g_1 = h_1 h g g_1, \quad h_1 \in H.$$

Como, $G_{i-1} \lhd G_i$, se tiene

$$g g_1 \in g G_{i-1} = G_{i-1} g.$$

Así,

$$x = h_1 h g_2 g, \quad \text{con} \quad g_2 \in G_{i-1},$$

o también,

$$x = h_1 h g_2 (h^{-1}h) g = h_1 h g_2 h^{-1}(hg) = h_1 h g_2 h^{-1} a. \tag{v}$$

Ahora, $g_2 h^{-1} \in G_{i-1}H = HG_{i-1}$, con lo que

$$g_2 h^{-1} = h_2 g_3, \quad h_2 \in H, \quad g_3 \in G_{i-1}.$$

Finalmente, sustituyendo en (v), $x = h_1 h h_2 g_3 a \in (HG_{i-1})a$.

Esto prueba la inclusión

$$a\,(HG_{i-1}) \subseteq (HG_{i-1})\,a.$$

Por simetría se obtiene la otra inclusión.

Por tanto $\widetilde{H}_{i-1}/H$ es subgrupo normal de $\widetilde{H}_i/H$. Como

$$\widetilde{H}_0 = G_0H = H, \qquad \text{y} \qquad \widetilde{H}_n = G_nH = G,$$

tenemos

$$\{1\} = \widetilde{H}_0/H \subset \widetilde{H}_1/H \subset \cdots \subset \widetilde{H}_{n-1}/H \subset \widetilde{H}_n/H = G/H$$

y los factores

$$\left(\widetilde{H}_i/H\right) / \left(\widetilde{H}_{i-1}/H\right) \cong \widetilde{H}_i/\widetilde{H}_{i-1} = (G_iH)/(G_{i-1}H) =$$

$$= G_i(G_{i-1}H)/(G_{i-1}H) \cong$$

$$\cong G_i/(G_i \cap G_{i-1}H) \cong (G_i/G_{i-1})/\left((G_i \cap G_{i-1}H)/G_{i-1}\right).$$

Como G_i/G_{i-1} es cíclico, también lo es $(G_i/G_{i-1})/\left((G_i \cap G_{i-1}H)/G_{i-1}\right)$, y en consecuencia $\left(\widetilde{H}_i/H\right) / \left(\widetilde{H}_{i-1}/H\right)$ es cíclico. Eliminando los términos repetidos obtenemos una serie cíclica de G/H.

(2) $\Longrightarrow$ (1): Sean

$$S : \{1\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = H$$

y

$$T : \{1\} = N_0 \subset N_1 \subset \cdots \subset N_{n-1} \subset N_m = G/H$$

series cíclicas de H y G/H respectivamente.

Cada N_i es de la forma G_i/H para $1 \leq i \leq m$, siendo G_i un subgrupo de G que contiene a H.

Como $N_m = G_m/H = G/H$, tenemos que $G_m = G$ y como $N_0 = H = G_0/H$, tenemos que $H = G_0$.

Además cada G_{j-1} es subgrupo normal de G_j por ser $N_{j-1} \lhd N_j$.

Por tanto,

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_n = H = G_0 \subset G_1 \subset \cdots \subset G_m = G,$$

es una serie de G cuyos factores son

- H_i/H_{i-1},
- $G_i/G_{i-1} \cong (G_i/H)/(G_{i-1}/H) = N_i/N_{i-1}$

y por lo tanto cíclicos.

■

Corolario 6.3.4 *Todo p-subgrupo es policíclico.*

DEMOSTRACIÓN. Sea G un p-grupo, con $o(G) = p^n$, p primo, $n \geq 1$. Probaremos el resultado por inducción en n.

En el caso $n = 1$, el grupo tiene orden primo, por lo que es simple y cíclico.

Supongamos cierto para el caso $n-1$, y sea $o(G) = p^n$. Entonces $\{1\} \neq Z(G)$, siendo $Z(G)$ subgrupo de G. Si $Z(G) = G$, entonces G es producto directo finito de grupos cíclicos, y por tanto policíclico. Si $Z(G) \neq G$, entonces $o(Z(G))$ y $o(G/Z(G))$ son estrictamente menores que p^n. Por hipótesis de inducción, ambos son policíclicos, de donde lo es G por la Proposición 6.3.3. ■

Otros ejemplos, derivados de esta Proposición son los siguientes.

Ejemplo 6.3.5 *Si p, q y r designan números primos y n un número natural, se verifica:*

1. *Todo grupo de orden $p^n q$ es policíclico.*
2. *Todo grupo de orden pqr es policíclico.*
3. *Todo grupo de orden $4p^n$ es policíclico.*
4. *Todo grupo de orden p^2q^2 es policíclico.*
5. *Todo grupo de orden p^3q^2 es policíclico.*

DEMOSTRACIÓN.

(1) La demostración la haremos por inducción sobre n.

Si $n = 0$, $o(G) = q$ y entonces G cíclico por el Corolario 1.5.16. Por tanto es policíclico.

Sea $n \geq 1$ y G un grupo de orden $p^n q$. Entonces por el Tercer Teorema de Sylow, G no es simple. Sea H un subgrupo normal propio de G. Como

$$o(H) = p^m q^i, \qquad 0 \leq m \leq n, \qquad i \in \{0, 1\}, \qquad 1 \leq m + i < n + 1,$$

se tiene $o(G/H) = p^{n-m} q^{1-i}$.

Si $i = 1$, como $m + i < n + 1$ entonces $m < n$, $n - m \geq 1$, de donde G/H es policíclico por el Ejemplo 6.3.4. Aplicando la hipótesis de inducción, tenemos que H es policíclico pues $o(H) = p^m q$, $m < n$. Por tanto, por la Proposición 6.3.3, tenemos que G es policíclico.

Si $i = 0$, el orden de H es p^m, entonces H es policíclico por el Ejemplo 6.3.4. Además como $1 \leq m + i = m$, se tiene $n - m < n$, luego por hipótesis de inducción G/H es policíclico ya que $o(G/H) = p^{n-m}q$. De nuevo se deduce que G es policíclico por la Proposición 6.3.3.

(2) Por el Tercer Teorema de Sylow sabemos que G posee un subgrupo normal propio H. Entonces $o(H)$ y $o(G/H)$ satisfacen que uno es primo y otro el producto de dos primos, luego por el apartado 1. se tiene que son policíclicos y por la Proposición 6.3.3 concluimos el resultado.

(3) Análoga al apartado (1).

(4) Análoga al apartado (1).

(5) Análoga al apartado (2).

■

Proposición 6.3.6 *Si G es un grupo policíclico, entonces G es finitamente generado.*

DEMOSTRACIÓN. Denotemos por n a la longitud de una serie cíclica de G. Haremos la demostración por inducción sobre n.

Si $n = 1$, tenemos una serie cíclica de la forma

$$\{1\} = G_0 \subset G_1 = G.$$

Como $G \cong G/\{1\}$ es cíclico, tendremos que G es cíclico y por tanto existe $a \in G$ tal que $G = \langle a \rangle$.

Sea ahora $n > 1$, y consideremos la serie cíclica

$$T : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

Si llamamos $G' = G_{n-1}$, entonces

$$\{1\} = G_0 \subset \cdots \subset G_{n-2} \subset G_{n-1} = G'$$

es una serie cíclica de G'. Así, G' es policíclico y tiene una serie de longitud $n - 1$. Por hipótesis de inducción, existe $S' = \{x_1, \ldots, x_m\} \subset G'$ tal que

$$G' = \langle S' \rangle.$$

Como T es una serie cíclica, el cociente $G/G' = G/G_{n-1}$ es un grupo cíclico, luego existe $x \in G_n = G$ tal que

$$G/G' = \langle xG' \rangle.$$

Consideremos ahora $S = \{x_1, \ldots, x_m, x\} \subset G$. Vamos a probar que $G = \langle S \rangle$.

Como $S = \{x_1, \ldots, x_m, x\} \subset G$, entonces $\langle S \rangle \subseteq G$. Recíprocamente, si $a \in G$, tenemos que $aG' \in G/G' = \langle xG' \rangle$. Luego existe $k \in \mathbb{N}$ tal que

$$aG' = (xG')^k = x^k G'.$$

Esto es,

$$x^{-k}a \in G' = \langle S' \rangle.$$

Es decir,

$$x^{-k}a = s_1^{h_1} \cdots s_l^{h_l}, \quad s_i \in S', \quad h_i \in \mathbb{Z}, \quad 1 \leq i \leq l.$$

Por tanto,

$$a = x^k s_1^{h_1} \cdots s_l^{h_l} \in \langle S \rangle.$$

Así, $G \subseteq \langle S \rangle$ y de ahí la igualdad.

■

Si G es abeliano el recíproco es cierto. Esto es lo que nos muestra la siguiente proposición.

Proposición 6.3.7 *Sea G un grupo abeliano. Las siguientes afirmaciones son equivalentes:*

1. *G es policíclico.*
2. *G admite un sistema finito de generadores.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2): Es la Proposición 6.3.6.
(2) $\Longrightarrow$ (1): Por el Teorema de Estructura de grupos abelianos finitamente generados, G es isomorfo a un producto directo finito de grupos cíclicos, y por tanto es policíclico.

■

Ejemplo 6.3.8 *El grupo $\mathbb{Q}$ de los números racionales con la operación suma es abeliano, pero no admite un sistema finito de generadores. En consecuencia, no es policíclico.*

De lo anterior se desprende el siguiente resultado, cuya demostración dejamos al lector.

Proposición 6.3.9 *Sea G un grupo que admite una serie de composición. Las siguientes afirmaciones son equivalentes:*

1. *G es policíclico.*
2. *Existe una serie de composición cíclica de G.*

3. *Toda serie de composición de G es cíclica.*

Ejemplo 6.3.10 *En virtud de la Proposición 6.3.9, si G no es abeliano, la equivalencia establecida en la Proposición 6.3.7 es falsa. Por ejemplo, observemos que S_5 es un grupo finitamente generado, y que*

$$\{1\} \lhd A_5 \lhd S_5$$

es una serie de composición. Pero A_5 es simple y no abeliano, y por tanto no es cíclico.

6.4. Conmutadores y subgrupos derivados

Procedemos en esta sección a introducir los elementos técnicos para estudiar los dos tipos de series más importantes.

Definición 6.4.1 *Sean G un grupo y H un subgrupo de G. Decimos que H es un subgrupo característico de G si $f(H) = H$ para todo $f \in Aut(G)$.*

Observación 6.4.2 *Nótese que H es característico si y sólo si $f(H) \subseteq H$ para todo $f \in Aut(G)$. En particular como la conjugación por un elemento es un automorfismo, todo subgrupo característico es normal.*

Definición 6.4.3 *(a) Dados dos elementos a y b de un grupo G, se llama conmutador de a y b al elemento*

$$[a, b] = a^{-1}b^{-1}ab \in G.$$

(b) Si H y K son dos subgrupos de G, se llama subgrupo conmutador de H y K, y lo denotaremos por $[H, K]$ al subgrupo generado por el conjunto $\{[h, k] : h \in H, k \in K\}$.

(c) Se llama derivado del grupo G a $G^1 = [G, G]$. Llamaremos segundo subgrupo derivado de G a $G^2 = [G^1, G^1]$ y por recurrencia, para cada natural positivo n, el n-ésimo derivado de G es $G^n = [G^{n-1}, G^{n-1}]$.

Observaciones 6.4.4 1. *Para cada natural $n > 1$, G^n es subgrupo de G^{n-1}, ya que para todo a, $b \in G^{n-1}$ se tiene que $[a, b] \in G^{n-1}$ y de ahí que el sistema generador de G^n está contenido en G^{n-1}.*

2. *$G^1 = \{1\}$ si y sólo si G es abeliano. Esta afirmación se obtiene del hecho que*

$$[a, b] = 1 \Longleftrightarrow ab = ba.$$

3. *Si* $f : G_1 \longrightarrow G_2$ *es un homomorfismo de grupos, se tiene que*

$$f([a,b]) = [f(a), f(b)] \qquad \text{para cada} \qquad a, b \in G,$$

ya que

$$f([a,b]) = f(a^{-1}b^{-1}ab) = f(a^{-1})f(b^{-1})f(a)f(b) =$$

$$= f(a)^{-1}f(b)^{-1}f(a)f(b) = [f(a), f(b)].$$

4. *Sea* $f : G_1 \longrightarrow G_2$ *un homomorfismo de grupos y sean* H *y* K *subgrupos de* G_1 *se tiene que*

$$f([H,K]) = [f(H), f(K)],$$

ya que por el apartado anterior, se tiene que las imágenes por f *de un sistema generador de* $[H,K]$ *es un sistema generador de* $[f(H), f(K)]$.

5. *Si* $f : G_1 \longrightarrow G_2$ *es epimorfismo, se tiene*

$$f(G_1^n) = G_2^n \qquad \text{para cada natural} \qquad n \geq 1.$$

Probaremos esta afirmación por inducción sobre n. *Si* $n = 1$, *por el apartado anterior, se tiene que*

$$f(G_1^1) = f([G_1, G_1]) = [f(G_1), f(G_1)] = [G_2, G_2] = G_2^1.$$

Si $n > 1$ *y aplicando la hipótesis de inducción se tiene que*

$$f(G_1^n) = f\left([G_1^{n-1}, G_1^{n-1}]\right) = [f(G_1^{n-1}), f(G_1^{n-1})] = [G_2^{n-1}, G_2^{n-1}] = G_2^n.$$

Proposición 6.4.5 *Sea* G *un grupo. Se verifica:*

1. G^n *es subgrupo característico de* G *para cada* $n \geq 1$.
2. G/G^1 *es un grupo abeliano.*
3. *Si* N *es un subgrupo normal de* G *y* G/N *es abeliano, entonces* $G^1 \subset N$.
4. *Todo subgrupo de* G *que contiene a* G^1 *es subgrupo normal de* G.

DEMOSTRACIÓN.

(1) Si $f \in Aut(G)$, en particular f es un epimorfismo. Entonces por la Observación 6.4.4(5), se tiene que $f(G^n) = G^n$ y de ahí que G^n sea un subgrupo característico de G.

(2) En el apartado (1) hemos visto que G^1 es un subgrupo característico de G, en particular es normal. Así G/G^1 es un grupo. Además para cualesquiera g_1G^1, $g_2G^1 \in G/G^1$, como $[g_2, g_1] \in G^1$, se tiene que

$$g_1G^1g_2G^1 = g_1g_2G^1 = g_1g_2[g_2, g_1]G^1 =$$

$$= g_1g_2g_2^{-1}g_1^{-1}g_2g_1G^1 = g_2g_1G^1 = g_2G^1g_1G^1.$$

(3) Basta ver que para cada a, $b \in G$ se tiene $[a, b] \in N$. Como G/N es abeliano se tiene que

$$abN = aNbN = bNaN = baN,$$

luego $(ba)^{-1}ab \in N$, es decir $[a, b] \in N$.

(4) Sea H subgrupo de G tal que $G^1 \subset H$. Entonces se tiene que H/G^1 es subgrupo del grupo abeliano G/G^1. Entonces H/G^1 es subgrupo normal de G/G^1 y por la Proposición 1.6.19 se tiene que H es subgrupo normal de G.

■

Lema 6.4.6 *Sean G_1 y G_2 dos grupos, H_1 y K_1 subgrupos de G_1, H_2 y K_2 subgrupos de G_2. Sea $G = G_1 \times G_2$. Entonces se verifica que*

$$[H_1 \times H_2,\ K_1 \times K_2] = [H_1,\ K_1] \times [H_2,\ K_2].$$

En particular $(G_1 \times G_2)^n = G_1^n \times G_2^n$.

DEMOSTRACIÓN. Un sistema generador de $[H_1 \times H_2, K_1 \times K_2]$ es

$$\{[(h_1, h_2), (k_1, k_2)] :\ h_1 \in H_1,\ h_2 \in H_2,\ k_1 \in K_1,\ k_2 \in K_2\}.$$

Como

$$[(h_1, h_2), (k_1, k_2)] = (h_1, h_2)^{-1}(k_1, k_2)^{-1}(h_1, h_2)(k_1, k_2) =$$

$$= (h_1^{-1}, h_2^{-1})(k_1^{-1}, k_2^{-1})(h_1, h_2)(k_1, k_2) =$$

$$= (h_1^{-1}k_1^{-1}h_1k_1, h_2^{-1}k_2^{-1}h_2k_2) = ([h_1, k_1], [h_2, k_2]),$$

y

$$\{([h_1, k_1], [h_2, k_2]) :\ h_1 \in H_1,\ h_2 \in H_2,\ k_1 \in K_1,\ k_2 \in K_2,\}$$

es un sistema generador de $[H_1, K_1] \times [H_2, K_2]$, tenemos que todo generador de $[H_1 \times H_2, K_1 \times K_2]$ es generador de $[H_1, K_1] \times [H_2, K_2]$. Por el mismo razonamiento tenemos que todo generador de $[H_1, K_1] \times [H_2, K_2]$ es generador de $[H_1 \times H_2, K_1 \times K_2]$ y de ahí la igualdad.

■

6.5. Grupos resolubles y nilpotentes

En esta sección estudiamos dos propiedades asociadas a series, cuya importancia histórica es obvia: la resolubilidad asociada a los trabajos de Abel, y la nilpotencia, asociada a la clasificación de álgebras de Lie de dimensión finita.

Definición 6.5.1 *Dado un grupo G, diremos que una serie de G es abeliana si todo factor de la serie es un grupo abeliano. Si G admite una serie abeliana diremos que G es un grupo resoluble.*

Ejemplos 6.5.2 *1. Todo grupo abeliano es resoluble ya que el cociente de un grupo abeliano es abeliano.*

2. Todo grupo policíclico es resoluble. Esto es obvio, pues un grupo policíclico admite una serie cuyos factores son cíclicos y por tanto abelianos.

3. No todo grupo resoluble es policíclico. Por ejemplo el grupo $\mathbb{Q}$ de los números racionales es resoluble por ser abeliano, sin embargo no es policíclico, como vimos en el Ejemplo 6.3.8.

Proposición 6.5.3 *Sea G un grupo que admite una serie de composición. Las siguientes afirmaciones son equivalentes:*

1. *G es resoluble.*
2. *G admite una serie de composición abeliana.*
3. *G admite una serie de composición cíclica.*
4. *Toda serie de composición de G es cíclica.*
5. *G es policíclico.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2): Sea

$$C : \{1\} = G_0 \subset G_1 \cdots \subset G_n = G$$

una serie de composición de G. Por hipótesis existe una serie abeliana de G,

$$S : \{1\} = H_0 \subset H_1 \cdots \subset H_m = G.$$

Por el Teorema de Schreir existen refinamientos equivalentes C' y S' de C y S respectivamente. Como C es serie de composición se tendrá que $C = C'$ y de ahí que C sea equivalente a S'. Veamos que S' también es serie abeliana.

Sea

$$H_{i-1} = K_0 \subset K_1 \cdots \subset K_l = H_i$$

el trozo de S' comprendido entre H_{i-1} y H_i.

Se tiene que H_{i-1} es subgrupo de K_j, ya que que H_{i-1} es subgrupo de H_i. Entonces por el Segundo Teorema de Isomorfía se tiene que

$$\frac{K_j}{K_{j-1}} \cong \frac{K_j/H_{i-1}}{K_{j-1}H_{i-1}}.$$

Por otra parte, $\dfrac{K_j}{H_{i-1}}$ es un grupo abeliano al ser subgrupo del grupo abeliano $\dfrac{H_i}{H_{i-1}}$. Entonces su cociente $\dfrac{K_j/H_{i-1}}{K_{j-1}/H_{i-1}}$ será abeliano. Así $\dfrac{K_j}{K_{j-1}}$ es abeliano. Esto implica que S' es abeliana.

Así la serie de composición C, al ser equivalente a S', es abeliana.

(2) $\Longrightarrow$ (3): Sea

$$T : \{1\} = M_0 \subset M_1 \subset \cdots \subset M_n = G$$

una serie de composición abeliana de G. Cada cociente M_i/M_{i-1} es abeliano y es simple. Por tanto $o(M_i/M_{i-1})$ es primo y de ahí que sea cíclico.

(3) $\Longrightarrow$ (4) $\Longrightarrow$ (5): Por la Proposición 6.3.9.

(5) $\Longrightarrow$ (1): Obvio.

■

Corolario 6.5.4 *Los ejemplos 6.3.5 son resolubles.*

Proposición 6.5.5 *Un grupo G es resoluble si y sólo si existe algún natural $n \geq 1$ tal que $G^n = \{1\}$.*

DEMOSTRACIÓN. Supongamos que exista $n \geq 1$ tal que $G^n = \{1\}$. Tomemos n el menor natural satisfaciendo esta condición. Esto implica que $G^i \neq G^{i-1}$ para cada $i \leq n$, pues si fuese $G^i = G^{i-1}$ para algún $i \leq n$, derivando $n - i$ veces en esta igualdad se obtendría

$$\{1\} = G^n = \left(G^i\right)^{n-i} = \left(G^{i-1}\right)^{n-i} = G^{n-1}$$

lo que contradice la elección de n.

Como $G^{n-i+1} = [G^{n-i}, G^{n-i}] \subset G^{n-i}$, se tiene que G^{n-i+1} es subgrupo de G^{n-i}. Además cada G^{n-i+1} es un subgrupo característico de G, y por tanto es normal en G. En particular, G^{n-i+1} es subgrupo normal de G^{n-i}. Entonces

$$D : \{1\} = G^n \subset G^{n-1} \subset \cdots \subset G^0 = G$$

es una serie, llamada serie derivada. Como G^j es el subgrupo derivado de G^{j-1} se tiene, por Proposición 6.4.5(2), que G^{j-1}/G^j es abeliano. Así D es una serie abeliana de G, de donde G es resoluble.

Recíprocamente, supongamos que G es resoluble y sea

$$S : \{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

una serie abeliana de G. Demostramos por recurrencia descendente sobre i que, llamando $G^0 = G$, se tiene $G^{n-i} \subseteq G_i$. Por tanto, $G^n \subseteq G_0 = \{1\}$ probará el resultado.

Para $i = n$ es obvio ya que $G^{n-n} = G^0 = G = G_n$. Sea ahora $i < n$. Como G_i es subgrupo normal de G_{i+1} y G_{i+1}/G_i es grupo abeliano, al ser S una serie abeliana, entonces, por Proposición 6.4.5(3), tenemos que

$$(G_{i+1})^1 \subset G_i.$$

Por hipótesis de recurrencia, $G^{n-(i+1)} \subset G_{i+1}$. Tomando derivados,

$$G^{n-i} = \left(G^{n-(i+1)}\right)^1 \subset (G_{i+1})^1 \subset G_i,$$

lo que termina el paso de inducción.

■

Proposición 6.5.6 *Sean G un grupo y H un subgrupo normal de G. Las siguientes afirmaciones son equivalentes:*

1. *G es resoluble.*
2. *H y G/H son resolubles.*

DEMOSTRACIÓN. (1) $\Longrightarrow$ (2) : Como $H \subset G$, se tiene que H^n es subgrupo de G^n para todo $n \geq 1$. Al ser G resoluble, por la Proposición 6.5.5, $G^m = \{1\}$ para cierto $m \geq 1$, y de ahí $H^m = \{1\}$. Luego H es resoluble por la Proposición 6.5.5.

Para la segunda afirmación, como la proyección canónica $\pi : G \longrightarrow G/H$ es un epimorfismo y $G^n = \{1\}$ para cierto $m \geq 1$, se tiene

$$(G/H)^n = \pi(G^n) = \pi(\{1\}) = \{\overline{1}\},$$

de donde G/H es resoluble por la Proposición 6.5.5.

(2) $\Longrightarrow$ (1): Supongamos que H y G/H son resolubles. Por la Proposición 6.5.5 existen n y m naturales tales que

$$H^n = \{1\}, \qquad (G/H)^m = H.$$

Entonces, como $\pi : G \longrightarrow G/H$ es epimorfismo, se tiene

$$\{\overline{1}\} = (G/H)^m = \pi(G^m) = G^m H/H = (G/H)^m,$$

luego $G^m H = H$ y de aquí $G^m \subset H$. Entonces $G^{m+n} \subset H^n = \{1\}$ y de ahí, por la Proposición 6.5.5 se tiene que G es resoluble.

■

Corolario 6.5.7 *Sean H y K dos subgrupos normales y resolubles de un grupo G. Entonces HK es un subgrupo normal y resoluble de G.*

DEMOSTRACIÓN. Se verifica que HK es un subgrupo normal de G. Por el Tercer Teorema de Isomorfía se tiene que

$$HK/K \cong H/(H \cap K).$$

Como H es resoluble, entonces por la Proposición 6.5.6, se tiene que $H/(H \cap K)$ es resoluble, de donde HK/K es resoluble. Como K es resoluble, por la Proposición 6.5.6 se tiene que HK es resoluble.

■

Corolario 6.5.8 *Sean G_1 y G_2 dos grupos. Entonces*

$$G_1 \times G_2 \text{ es resoluble si y sólo si } G_1 \text{ y } G_2 \text{ son resolubles.}$$

DEMOSTRACIÓN. Si $G_1 \times G_2$ es resoluble, existe $n \geq 1$ tal que $(G_1 \times G_2)^n = \{(1,1)\}$. Entonces, en virtud del Lema 6.4.6 se tiene que $(G_1^n \times G_2^n) = \{(1,1)\}$ y de ahí que

$$G_1^n = \{1\}, \qquad G_2^n = \{1\}.$$

Por tanto G_1 y G_2 son grupos resolubles.

Recíprocamente, supongamos que G_1 y G_2 son grupos resolubles y sean m, n positivos tales que $G_1^n = \{1\}$ y $G_2^m = \{1\}$. Entonces si $r = \text{máx}\{m,n\}$ se tiene

$$\{1\} \subset G_1^r \subseteq G_1^m = \{1\}, \qquad \{1\} \subset G_2^r \subseteq G_2^n = \{1\}.$$

Entonces en virtud del Lema 6.4.6 se tiene que

$$(G_1 \times G_2)^r = (G_1^r \times G_2^r) = \{(1,1)\}$$

y $G_1 \times G_2$ es resoluble.

■

Ejemplo 6.5.9 *El grupo S_3 es resoluble. Basta observar que $o(S_3) = 6 = 2 \cdot 3$ y aplicar el Corolario 6.5.4.*

Teorema 6.5.10 (Teorema de Abel) *S_n no es resoluble si $n \geq 5$.*

DEMOSTRACIÓN. Si S_n es resoluble con $n \geq 5$, como es finito entonces tenemos que S_n es policíclico. Por tanto A_n sería un grupo policíclico. Pero al ser A_n un subgrupo simple, tendríamos que A_n es cíclico, y esto es contradictorio con el hecho de que A_n no es abeliano.

■

Finalmente, a título informativo, incluimos una versión del Teorema de Feit-Thomson, que establece una condición de suficiencia importante para la resolubilidad de grupos finitos.

Teorema 6.5.11 (Teorema de Feit-Thomson) *Todo grupo finito de orden impar es resoluble.*

Para terminar, estudiamos una clase restringida de la clase de grupos resolubles, asociada a una serie de subgrupos característicos muy particular.

Dado G un grupo, definimos recurrentemente una colección $\{Z_n\}_{n\geq 0}$ de subgrupos, como sigue:

- $Z_0 = \{1\}$.
- $Z_1 = Z(G)$. Observemos que $Z_1 \lhd G$.
- Para todo $k > 1$, Z_k es el único subgrupo de G conteniendo Z_{k-1}, y tal que $Z_k/Z_{k-1} = Z\left(G/Z_{k-1}\right)$. Como $Z\left(G/Z_{k-1}\right) \lhd G/Z_{k-1}$, se tiene que $Z_k \lhd G$.

Definición 6.5.12 *La serie ascendente*

$$Z(G) : \{1\} \subseteq Z_1 \subseteq Z_2 \subseteq \cdots \subseteq Z_k \subseteq \cdots$$

se denomina serie central superior.

Observación 6.5.13 *Para todo $k \geq 1$ se tiene*

$$Z_k = \{x \in G : [x, y] \in Z_{k-1},\ \forall y \in G\}.$$

Definición 6.5.14 *Sea G un grupo. Si existe $n \geq 1$ tal que $Z_n = G$, decimos que G es nilpotente, y si n el elemento natural mínimo que verifica esta propiedad, se dice que G es de clase de nilpotencia n.*

Lema 6.5.15 *Se tiene que:*

(a) Todo grupo nilpotente es resoluble.

(b) Todo grupo abeliano es nilpotente.

DEMOSTRACIÓN. Si el grupo es nilpotente existe una serie central superior de la forma

$$Z(G) : \{1\} \subseteq Z_1 \subseteq Z_2 \subseteq \cdots \subseteq Z_n = G.$$

Los factores de dicha serie son abelianos ya que

$$Z_k/Z_{k-1} = Z\left(G/Z_{k-1}\right).$$

Por tanto, la serie es abeliana, de donde G es resoluble.

■

Observación 6.5.16 *No todo grupo resoluble es nilpotente. Por ejemplo para S_3 se tiene la serie*

$$\{1\} \lhd A_3 \lhd S_3.$$

Esta serie es abeliana ya que $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ y $S_3/A_3 = \mathbb{Z}/2\mathbb{Z}$. Por tanto S_3 es resoluble. Sin embargo S_3 no es nilpotente ya que $Z(S_n) = \{1\}$ para todo $n \geq 3$.

Observación 6.5.17 *1. No todo grupo nilpotente es policíclico. Por ejemplo el grupo abeliano de los números racionales es nilpotente, y sin embargo no es policíclico como hemos visto anteriormente.*

2. No todo grupo policíclico es nilpotente. Por ejemplo S_3 es un grupo policíclico y sin embargo no es nilpotente como hemos visto.

Otra clase de grupos nilpotentes es la de los p-grupos.

Lema 6.5.18 *Sea G un grupo. Si $G/Z(G)$ es nilpotente, entonces G es nilpotente.*

DEMOSTRACIÓN. Consideremos la serie central superior de $G/Z(G)$

$$\{\overline{1}\} \subset Z_1(G/Z(G)) \subset \cdots \subset Z_k(G/Z(G)) = G/Z(G).$$

Para cada $1 \leq i \leq k$ existe un único subgrupo normal de G, que denotamos Z_i', conteniendo a $Z(G)$, y tal que $Z_i'/Z(G) \cong Z_i(G/Z(G))$. Observemos que, en particular, $Z_k' = G$. Vamos a probar por recurrencia en i que $Z_i' = Z_{i+1}(G)$. Visto esto, por la observación anterior concluiremos que G es nilpotente.

En el caso $i = 0$, como $\{\overline{1}\} = Z_0'/Z(G)$, está claro que $Z_0' = Z_1(G)$.

Supuesto cierto para un $i < k$, vamos a probar la afirmación para $i + 1$. Para ello observemos que

$$Z_{i+1}'/Z_{i+1}(G) \cong Z_{i+1}'/Z_i' \cong (Z_{i+1}'/Z(G))/(Z_i'/Z(G)) \cong$$
$$\cong Z_{i+1}(G/Z(G))/Z_i(G/Z(G)) \cong Z\left((G/Z(G)/Z_i(G/Z(G))\right) \cong$$
$$\cong Z\left((G/Z(G)/(Z_{i+1}(G)/Z(G))\right) \cong Z(G/Z_{i+1}(G)) \cong Z_{i+2}(G)/Z_{i+1}(G).$$

Por lo tanto, $Z_{i+1}' = Z_{i+2}(G)$, probando el paso de recurrencia.

■

Proposición 6.5.19 *Todo p-grupo es nilpotente.*

DEMOSTRACIÓN. Si G es un p-grupo, entonces $o(G) = p^n$ para algún $n \in \mathbb{N}$. Haremos la demostración por inducción en n.

Para $n = 1$, el grupo es cíclico, de donde abeliano, y por tanto $Z(G) = G$.

Supongamos cierto para todo $k < n$, y sea $o(G) = p^n$. Por el Corolario 5.2.5 se tiene

$$\{1\} \neq Z(G) \lhd G.$$

Claramente $G/Z(G)$ es un p-grupo con $o(G/Z(G)) < p^n$. Por hipótesis de inducción $G/Z(G)$ es nilpotente, de donde G es nilpotente por Lema 6.5.18.

■

Observación 6.5.20 *Sea G un grupo y H un subgrupo normal de G tales que H y G/H son nilpotentes. Esto no implica que G sea nilpotente. Basta observar que*

$$A_3 \lhd S_3, \qquad \text{con} \qquad A_3 \cong \mathbb{Z}/3\mathbb{Z} \quad \text{nilpotente}$$

y

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}, \text{ nilpotente}$$

y sin embargo hemos visto que S_3 no es nilpotente.

Lema 6.5.21 *Sean G_1 y G_2 grupos entonces*

$$G_1 \times G_2 \text{ es nilpotente si y sólo si } G_1 \text{ y } G_2 \text{ son nilpotentes.}$$

DEMOSTRACIÓN. Basta tener en cuenta que

$$Z_k(G_1 \times G_2) = Z_k(G_1) \times Z_k(G_2).$$

■

Notación 6.5.22 *Sea G un grupo. Denotaremos*

$$\gamma_1(G) := G, \qquad \gamma_2(G) := [\gamma_1(G), G],$$

y por recurrencia

$$\gamma_{i+1}(G) := [\gamma_i(G), G], \qquad i \geq 0.$$

Lema 6.5.23 *Sean G_1 y G_2 grupos, y sea $f : G_1 \longrightarrow G_2$ un homomorfismo. Entonces, para cada $i \in \mathbb{N}$ se verifica*

$$f(\gamma_i(G)) = \gamma_i(f(G)).$$

DEMOSTRACIÓN. La demostración la haremos por inducción sobre i.

Si $i = 1$, aplicando la Observación 6.4.4(3) se tiene

$$f(\gamma_1(G)) = f(G) = \gamma_1(f(G)).$$

Si $i > 1$ se tiene, aplicando la hipótesis de recurrencia y la Observación 6.4.4(3),

$$f(\gamma_i(G_1)) = f[\gamma_{i-1}(G_1), G_1] = [f(\gamma_{i-1}(G_1)), f(G_1)] =$$

$$= [\gamma_{i-1}(f(G_1)), f(G_1)] = \gamma_i(f(G_1)).$$

■

Lema 6.5.24 *Sea G un grupo. Se verifica que:*

1. *$\gamma_i(G)$ es subgrupo característico para todo $i \in \mathbb{N}$. En particular $\gamma_i(G)$ es un subgrupo normal de G.*
2. *$\gamma_2(G) = [\gamma_1(G), G] = G^1$, y $\gamma_{i+1}(G)$ es subgrupo de $\gamma_i(G)$ para todo $i \in \mathbb{N}$.*

DEMOSTRACIÓN. (1) Es consecuencia directa de la Proposición 6.5.23.

(2) Por el apartado (1), bastará demostrar que $\gamma_{i+1}(G) \subseteq \gamma_i(G)$. Para ello dados $a \in \gamma_i(G)$, $b \in G$, veamos que $[a, b] \in \gamma_i(G)$. Como $\gamma_i(G) \lhd G$, se tiene $b^{-1}ab \in \gamma_i(G)$. Por tanto $a^{-1}b^{-1}ab \in \gamma_i(G)$. Así $[a, b] \in \gamma_i(G)$.

■

Lema 6.5.25 *Sea H un subgrupo G sea K un subgrupo de H tal que K es normal en G. Entonces $[H, K]$ es subgrupo de K si y sólo si H/K es subgrupo de $Z(G/K)$.*

DEMOSTRACIÓN. Dados $h \in H$ y $g \in G$ se tiene que

$$hgK = ghK \iff [h, g] \in K.$$

Entonces podemos afirmar que

$$(hK)(gK) = (gK)(hK) \iff [H, K] \text{ es subgrupo de } K.$$

Así obtenemos el resultado.

■

Corolario 6.5.26 *Para todo $i \in \mathbb{N}$ se tiene*

$$\gamma_i(G)/\gamma_{i+1}(G) \text{ es subgrupo de } Z(G/\gamma_{i+1}(G)).$$

DEMOSTRACIÓN. Por definición tenemos que $[\gamma_i(G), G] = \gamma_{i+1}(G)$. Ahora estamos en condiciones de aplicar el Lema 6.5.25 y de ahí obtenemos el resultado. ∎

Teorema 6.5.27 *Sea G un grupo. Entonces existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$ si y sólo si $\gamma_{n+1}(G) = \{1\}$. Más aún, en tal caso $\gamma_{i+1}(G)$ es subgrupo de $Z_{n-i}(G)$ para todo $i \in \mathbb{N}$.*

DEMOSTRACIÓN. Supongamos que existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$. Probaremos que γ_{i+1} es subgrupo de $Z_{n-i}(G)$ por inducción sobre i. Para ello bastará demostrar que $\gamma_{i+1} \subseteq Z_{n-i}(G)$.

Si $i = 0$, entonces $\gamma_1(G) = G = Z_n(G)$.

Sea $i > 0$ y supongamos $\gamma_{i+1} \subseteq Z_{n-i}(G)$. Entonces

$$\gamma_{i+2}(G) = [\gamma_{i+1}(G), G] \subseteq [Z_{n-i}(G), G] \subseteq Z_{n-i-1}(G),$$

aplicando la hipótesis de inducción en la primera inclusión y el Lema 6.5.25 en la segunda. Esto prueba el paso de inducción. En particular para $i = n$,

$$\gamma_{n+1}(G) \subseteq Z_0(G) = \{1\}.$$

Recíprocamente, supongamos $\gamma_{n+1}(G) = \{1\}$. Probaremos que $\gamma_{n+1-j}(G)$ es subgrupo de $Z_j(G)$, por inducción sobre j. Para ello bastará probar que $\gamma_{n+1-j}(G) \subseteq Z_j(G)$.

Si $j = 0$, $\gamma_{n+1}(G) = \{1\} \subseteq G = Z_0(G)$.

Sea $j > 0$, y supongamos $\gamma_{n+1-j}(G) \subseteq Z_j(G)$. Consideremos el homomorfismo de grupos

$$\varphi : G/\gamma_{n+1-j}(G) \longrightarrow G/Z_j(G),$$

donde $\ker(\varphi) = \dfrac{Z_j(G)}{\gamma_{n+1-j}(G)}$.

Por el Primer Teorema de Isomorfía tenemos

$$\frac{G/\gamma_{n+1-j}(G)}{Z_j(G)/\gamma_{n+1-j}(G)} \cong Im(\varphi).$$

Así por el Segundo Teorema de Isomorfía tenemos que $G/Z_j(G) \cong Im(\varphi)$. Por tanto φ es un epimorfismo.

Por otro lado, como $\gamma_{n+1-j}(G) = [\gamma_{n-j}(G), G]$, por el Lema 6.5.25 se tiene que

$$\frac{\gamma_{n-j}(G)}{\gamma_{n+1-j}(G)} \text{ es subgrupo de } Z\left(G/\gamma_{n+1-j}(G)\right).$$

Por tanto, como φ es epimorfismo, se tiene

$$\varphi\left(\frac{\gamma_{n-j}(G)}{\gamma_{n+1-j}(G)}\right) \subseteq Z\left(G/Z_j(G)\right),$$

es decir,

$$\frac{\gamma_{n-j}(G)Z_j(G)}{Z_j(G)} \subseteq Z\left(G/Z_j(G)\right) = \frac{Z_{j+1}(G)}{Z_j(G)}.$$

Así

$$\gamma_{n-j}(G) \subseteq \gamma_{n-j}(G)Z_j(G) \subseteq Z_{j+1}(G),$$

lo que completa el paso de inducción.

En particular para $j = n$, tenemos $G = \gamma_1(G)$ es subgrupo de $Z_n(G)$, luego $G = Z_n(G)$.

■

Corolario 6.5.28 *Sea G un grupo nilpotente de clase n. Entonces*

1. *Si H es un subgrupo de G, entonces H es nilpotente de clase menor o igual que n.*
2. *Si H es subgrupo normal de G, entonces G/H es nilpotente de clase menor o igual que n.*

DEMOSTRACIÓN.

(1) Demostraremos en primer lugar, por inducción sobre i, que

$$\gamma_i(H) \subseteq \gamma_i(G) \text{ para cada } i \in \mathbb{N}.$$

Si $i = 1$, $\gamma_1(H) = H \subseteq G = \gamma_1(G)$.
Sea $i > 1$, entonces

$$\gamma_i(H) = [\gamma_{i-1}(H), H] \subseteq [\gamma_{i-1}(G), G] = \gamma_i(G),$$

siendo cierta la inclusión $[\gamma_{i-1}(H), H] \subseteq [\gamma_{i-1}(G), G]$ porque $H \subseteq G$ y, por hipótesis de inducción, se tiene $\gamma_{i-1}(H) \subseteq \gamma_{i-1}(G)$.

Ahora probamos (1). Como G es nilpotente de clase n, por el Teorema 6.5.27, existe $n \geq 1$ tal que $\gamma_n(G) = \{1\}$.

Por lo anterior,

$$\gamma_n(H) \subseteq \gamma_n(G) = \{1\},$$

luego $\gamma_n(H) = \{1\}$ y H es nilpotente de clase menor o igual que n.

(2) Como $\pi : G \longrightarrow G/H$ es un epimorfismo, se tiene

$$\gamma_i(G/H) = \gamma_i(\pi(G)) = \pi(\gamma_i(G)).$$

Así, como G es nilpotente de clase n, $\gamma_n(G) = \{1\}$. Luego

$$\gamma_n(G/H) = \pi\left(\gamma_n(G)\right) = \{\overline{1}\}.$$

Por tanto, G/H es nilpotente de clase menor o igual que H.

■

Finalmente, damos una caracterización de los grupos nilpotentes finitos.

Lema 6.5.29 *Sea G un grupo nilpotente. Si H es un subgrupo propio de G, entonces $H \subsetneqq N_G(H)$.*

DEMOSTRACIÓN. Como H es subgrupo, $Z_0 = \{1\} \subseteq H$. Sea n el mayor natural tal que $Z_n \subseteq H$. Notemos que existe un tal n, puesto que G es nilpotente y H es un subgrupo propio. Sea $a \in Z_{n+1} \setminus H$. Entonces, como $Z_{n+1}/Z_n \cong Z(G/Z_n)$, para todo $h \in H$ se tiene $(ah)Z_n = (ha)Z_n$ en G/Z_n. Así, $ah = h'ha$ para cierto $h' \in Z_n \subseteq H$, de donde $aha^{-1} \in H$ para todo $h \in H$. Por lo tanto, $a \in N_G(H) \setminus H$.

■

Teorema 6.5.30 *Un grupo finito es nilpotente si y sólo si es el producto directo de sus subgrupos de Sylow.*

DEMOSTRACIÓN. Si $G \cong P_1 \times \cdots \times P_r$, siendo P_i los p_i-subgrupos de Sylow de G, entonces G es nilpotente por la Proposición 6.5.19 y el Lema 6.5.21.

Recíprocamente, sea G nilpotente, sea p un número primo que divida a $o(G)$, y sea P un p-subgrupo de Sylow de G. Como $P \subset G$, se tiene que $P \subset N_G(P)$ por el Lema 6.5.29. Como P es un subgrupo de Sylow de G, también lo es de $N_G(P)$, de donde es el único p-subgrupo de Sylow de $N_G(P)$. Si $x \in N_G\left(N_G(P)\right)$, se tiene $xN_G(P)x^{-1} = N_G(P)$. Así, xPx^{-1} es un p-subgrupo de $N_G(P)$, de donde $xPx^{-1} = P$, lo que implica que $x \in N_G(P)$. De este modo,

$$N_G\left(N_G(P)\right) \subseteq N_G(P),$$

luego

$$N_G\left(N_G(P)\right) \subseteq N_G(P) \subseteq N_G\left(N_G(P)\right),$$

de donde $N_G\left(N_G(P)\right) = N_G(P)$. Por Lema 6.5.29, $N_G(P) = G$, lo que nos dice que P es un p-subgrupo normal de G. Entonces el resultado se obtiene por el Teorema 5.3.15.

■

6.6. Ejercicios

1. Demostrad que $\mathbb{Q}$ no tiene subgrupos característicos distintos de $\{0\}$ y $\mathbb{Q}$.

2. Demostrad que todo grupo finito admite una serie de composición.

3. Sean $G.H$ dos grupos que admiten series de composición de igual longitud, con factores dos a dos isomorfos. ¿Son isomorfos G y H?

4. Demostrad que el grupo abeliano $(\mathbb{Q}, +)$ no es policíclico.

5. Para cada natural $n \geq 3$, demostrad que el grupo diédrico D_n es policíclico. Construid una serie de composición del grupo D_6.

6. Probad que si G es simple y resoluble entonces G es cíclico de orden primo.

7. Sea G un grupo, y sean K, H subgrupos normales de G. Probad:

   a) Si G/H y G/K son resolubles, entonces $G/(H \cap K)$ es resoluble.

   b) Si G/H y G/K son nilpotentes, entonces $G/(H \cap K)$ es nilpotente.

8. Sea G grupo finito. Ved que son equivalentes:

   a) G es nilpotente.

   b) $Z(G/H) \neq \{1\}$ para todo subgrupo normal $H \neq G$ de G.

9. Demostrad que:

   a) $S_n^1 = A_n$.

   b) $Q_8^1 = \{I, -I\}$.

10. Demostrad que S_3 y S_4 son grupos resolubles y calculad una serie derivada de cada uno de ellos.

Capítulo 7

Grupos libres. Presentaciones de grupos

El objetivo de este capítulo es establecer la noción de grupo dado por generadores y relaciones, así como considerar el problema de isomorfismo entre diversas presentaciones de un grupo.

7.1. Coproducto de grupos. Grupo libre

Definición 7.1.1 *Sea G un grupo y $\{G_i\}_{i\in I}$ una colección de subgrupos de G. Diremos que la familia $\{G_i\}_{i\in I}$ genera G, si todo elemento $g \in G$ puede escribirse como*

$$g = x_1 \cdots x_n, \qquad con \qquad x_i \in G_i, \qquad i \in I.$$

Sea G un grupo, y sea $\{G_i\}_{i\in I}$ una colección de subgrupos de G que generan G. Entonces para todo $g \in G$ existen $x_j \in G_{i_j}$, $i_j \in I$ de modo que

$$g = x_1 \cdots x_n.$$

Si agrupamos términos contiguos que pertenezcan al mismo subgrupo G_j, esto significa que $g = 1$ ó $g = x_1 \cdots x_n$ con $x_i \neq 1$ y x_i, x_{i+1} no pertenecen al mismo subgrupo. Llamamos a esta expresión *presentación en forma canónica del elemento g.*

Definición 7.1.2 *Sea G un grupo, y $\{G_i\}_{i\in I}$ una familia de subgrupos de G generando G. Si para todo $g \in G$ la presentación en forma canónica es única, diremos que G es el coproducto de la familia $\{G_i\}_{i\in I}$, denotado $G = \coprod_{i\in I} G_i$.*

Recíprocamente, dada una familia de grupos $\{G_i\}_{i\in I}$, veamos cómo siempre es posible definir un coproducto de la familia.

Definición 7.1.3 *1. Para $k \geq 1$, una palabra de longitud k es una k-upla $(x_1, \ldots, x_k)$ donde cada x_i pertenece a algún G_j, x_i, x_{i+1} no pertenecen al mismo G_j, y ningún x_i es el neutro de un subgrupo G_j.*

2. Dos palabras $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_l)$ son iguales si $k = l$ y $x_i = y_i$ para cada $1 \leq i \leq k$.

3. Denotaremos por $(-)$ la palabra vacía o de longitud cero.

Consideremos G el conjunto de palabras de longitud finita $n \in \mathbb{N}$, que se pueden escribir usando los elementos de los grupos G_i como letras. Es decir

$$G = \{(x_1, \ldots, x_n) : n \in \mathbb{N},\ x_i \in G_{ji},\ x_i \neq 1,\ j_i \in I,\ j_i \neq j_{i+1}\} \cup \{(-)\}.$$

Definimos en G la siguiente operación:

$$(x_1, \ldots, x_k)(y_1, \ldots, y_l) =$$

$$\begin{cases} (1) & (x_1, \ldots, x_k) & \text{si} & (y_1, \ldots, y_l) = (-) \\ (2) & (y_1, \ldots, y_l) & \text{si} & (x_1, \ldots, x_r) = (-) \\ (3) & (x_1, \ldots, x_k, y_1, \ldots, y_l) & \text{si} & x_k \in G_i,\ y_1 \in G_j,\ i \neq j \\ (4) & (x_1, \ldots, x_k y_1, \ldots, y_l) & \text{si} & x_k, y_1 \in G_i,\ x_k y_1 \neq 1 \\ (5) & (x_1, \ldots, x_{k-1}, y_2, \ldots, y_l) & \text{si} & x_k y_1 = 1. \end{cases}$$

Se entiende que en el caso quinto de la definición, nos volvemos a plantear si x_{k-1} e y_2 pertenecen a un mismo subgrupo G_i, en cuyo caso se agrupan o si su producto es el neutro, y así sucesivamente, quedando

$$(x_1, \ldots, x_r, z_1, \ldots, z_t, y_s, \ldots, y_l),$$

donde $\quad 1 \leq r < k, \quad 1 \leq s < l, \quad 1 \leq r + t + (l - s) < k + l.$

La operación anterior definida en G verifica:

- Es asociativa.
- $(-)$ es el elemento neutro.
- Todo elemento $(x_1, \ldots, x_n)$ tiene inverso $(x_1, \ldots, x_n)^{-1} = (x_n^{-1}, \ldots, x_1^{-1})$.

Por tanto podemos afirmar que G es un grupo respecto de la operación definida anteriormente.

Asimismo para todo $i \in I$, la aplicación $\alpha_i : G_i \longrightarrow G$, definida como

$$\alpha_i(x) = \begin{cases} (x) & \text{si} \quad x \neq 1 \\ (-) & \text{si} \quad x = 1, \end{cases}$$

es un monomorfismo de grupos: si $x \in \ker(\alpha_i)$, entonces se tiene que $\alpha_i(x) = (-)$, es decir, $(x) = (-)$, de donde $x = 1$.

Así, por el Primer Teorema de Isomorfía, se tiene

$$G_i \cong \alpha_i(G_i) \subseteq G,$$

es decir, G contiene una familia de subgrupos isomorfos a los subgrupos G_i.

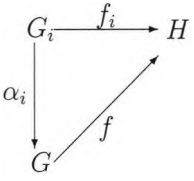
Dado $g \in G$ con $g \neq 1$, se tiene

$$g = (x_1, \ldots, x_n) = (x_1) \cdots (x_n) = \alpha_{i_1}(x_1) \cdots \alpha_{i_n}(x_n),$$

donde cada x_i pertenece a algún $\alpha_{i_j}(G_{i_j})$, ningún x_i es el neutro de G y x_i, x_{i+1} no pertenecen al mismo $\alpha_{i_j}(G_{i_j})$. Claramente, la expresión anterior es única. Así, $G = \coprod_{i \in I} \alpha_i(G_i)$.

El coproducto de una familia de grupos queda caracterizado mediante una propiedad universal.

Teorema 7.1.4 *Sea $\{G_i\}_{i \in I}$ una familia de grupos, sea $G = \coprod_{i \in I} \alpha_i(G_i)$ su coproducto donde $\alpha_i : G_i \longrightarrow G$ son los monomorfismos canónicos. Dado un grupo H cualesquiera, y una familia de homomorfismos $f_i : G_i \longrightarrow H$, existe un único morfismo $f : G \longrightarrow H$ tal que, para todo $i \in I$, $f \circ \alpha_i = f_i$, esto es, el diagrama*



conmuta.

DEMOSTRACIÓN. Dado $g = (x_1, \ldots, x_n) \in G$, $g \neq 1$ con $x_i \in G_{j_i}$, definimos

$$f(x_1, \ldots, x_n) = f_{i_1}(x_1) \cdots f_{i_n}(x_n).$$

Para $g = 1$, definimos $f((-)) = 1$.

Se verifica que:

- f está bien definido ya que la expresión de g es única.
- Es obvio que f es un homomorfismo.

- El diagrama conmuta ya que, para cada G_i, tenemos

$$f_i(x_i) = f((x_i)) = f \circ \alpha_i(x_i).$$

- Veamos la unicidad: sea $g : G \longrightarrow H$ otro homomorfismo conmutando dicho diagrama. Para cualquier $i \in I$, si $x_i \in G_i$, se tiene

$$g((x_i)) = g \circ \alpha_i(x_i) = f_i(x_i) = f((x_i)).$$

Como g es homomorfismo, se tiene, para $(x_1, \ldots, x_n) \in G$,

$$g(x_1, \ldots, x_n) = g((x_1) \cdots (x_n)) = g((x_1)) \cdots g((x_n)) =$$

$$= f((x_1)) \cdots f((x_n)) = f(x_1, \ldots, x_n).$$

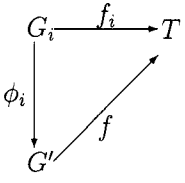
Como G es el conjunto de todas estas palabras, concluimos que $g = f$.

■

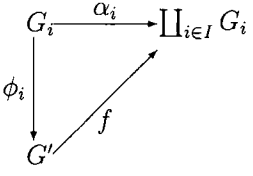
El coproducto queda caracterizado por la propiedad universal del Teorema 7.1.4, como veremos a continuación.

Corolario 7.1.5 *Sea G' un grupo y $\phi_i : G_i \longrightarrow G'$ una familia de homomorfismos de modo que $\{G', \phi\}$ verifiquen la propiedad del Teorema 7.1.4. Entonces $G' \cong G$.*

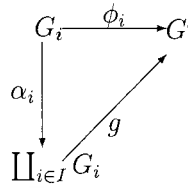
DEMOSTRACIÓN. Sea $(G', \{\phi_i\}_{i \in I})$ un grupo con una familia de homomorfismos $\phi_i : G_i \longrightarrow G'$ tales que para cualquier grupo T con morfismos $f_i : G_i \longrightarrow T$ existe $f : G' \longrightarrow T$ conmutando el diagrama



En particular, para $T = \coprod_{i \in I} G_i$, $f_i = \alpha_i$ tenemos



Como el coproducto tiene la misma propiedad por el Teorema 7.1.4, existe un único $g : \coprod_{i \in I} G_i \longrightarrow G'$ conmutando el diagrama



Para probar que $\coprod_{i\in I} G_i$ y G' son isomorfos, basta probar que $f \circ g$ y $g \circ f$ son la identidad.

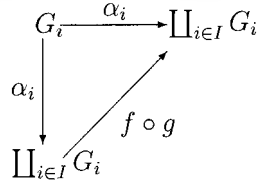
Se tiene que

$$f \circ \phi_i = \alpha_i, \qquad g \circ \alpha_i = \phi_i.$$

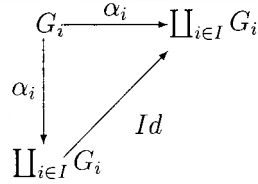
Así

$$(f \circ g) \circ \alpha_i = f \circ (g \circ \alpha_i) = f \circ \phi_i = \alpha_i.$$

Por tanto se tiene el siguiente diagrama conmutativo



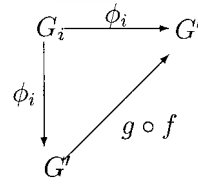
También se tiene el siguiente diagrama conmutativo



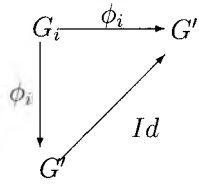
Por la unicidad, debida al Teorema 7.1.4, se tiene que $f \circ g = Id$. También se tiene que

$$(g \circ f) \circ \phi_i = g \circ (f \circ \phi_i) = g \circ \alpha_i = \phi_i.$$

Por tanto se tiene el siguiente diagrama conmutativo



También se tiene el siguiente diagrama conmutativo



Pero como el homomorfismo es único por hipótesis, se tiene que $g \circ f = Id$, luego $\coprod_{i \in I} G_i \cong G'$.

■

El ejemplo más importante de coproducto es el llamado grupo libre asociado a un conjunto. Su existencia y propiedades nos permitirán establecer formalmente la noción de presentación de un grupo.

Sea X un conjunto no vacío, $X = \{x_i\}_{i \in I}$. Para cada x_i consideramos el conjunto

$$G_{x_i} = \{x_i^n : n \in \mathbb{Z}\}.$$

Definimos en G_{x_i} la siguiente operación:

$$x_i^n x_i^m := x_i^{n+m}.$$

Se tiene que:

- El elemento neutro es $x_i^0 := 1$.
- Para cada x_i^n definimos su inverso $(x_i^n)^{-1} := x_i^{-n}$.

Por tanto G_i con la operación así definida tiene estructura de grupo.

Observación 7.1.6 *Observemos que* $G_{x_i} \cong \mathbb{Z}$.

Definición 7.1.7 *Sea* $X = \{x_i\}_{i \in I}$ *un conjunto no vacío. Definimos el grupo libre sobre* X*, denotado* $F(X)$*, como*

$$F(X) := \coprod_{i \in I} G_{x_i}.$$

Llamamos base de $F(X)$ *al conjunto* X*, y rango de* $F(X)$ *a* $\operatorname{card}(X)$.

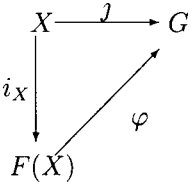
Observación 7.1.8 *Observemos que* $F(X) \cong \coprod_{x \in X} \mathbb{Z}$. *Por tanto*

$$F(X)^{ab} = F(X)/F(X)' \cong \bigoplus_{x \in X} \mathbb{Z},$$

esto es, el grupo abeliano libre sobre X*. Pero notemos que* $F(X)$ *es abeliano si y sólo si* $\operatorname{card}(X) = 1$.

El grupo libre sobre un conjunto, por ser un coproducto, se caracteriza por una propiedad universal.

Teorema 7.1.9 *Sea X un conjunto no vacío, sea G un grupo, y sea $j : X \longrightarrow G$ una aplicación (de conjuntos). Entonces existe un único homomorfismo $\varphi : F(X) \longrightarrow G$ conmutando el siguiente diagrama*



donde

$$\begin{array}{rcl} j : X & \longrightarrow & F(X) \\ x_i & \longmapsto & (x_i) \end{array}$$

DEMOSTRACIÓN. Sea $w \in F(X)$ con $w \neq 1$. Entonces $w = x_1^{n_1} \cdots x_k^{n_k}$ con $x_i \in X$, y por tanto $x_i \in G_{x_i}$.

Definimos

$$\varphi(w) = j(x_1)^{n_1} \cdots j(x_k)^{n_k}.$$

Probar que es un homomorfismo bien definido y único es análogo al argumento del Teorema 7.1.4.

■

Corolario 7.1.10 *La propiedad universal caracteriza al grupo libre.*

DEMOSTRACIÓN. Análoga a la del Corolario 7.1.5.

■

Como consecuencia, tenemos el siguiente resultado, esencial para manipular grupos.

Teorema 7.1.11 *Todo grupo es cociente de un grupo libre.*

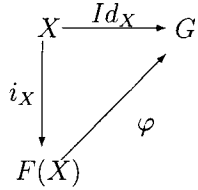
DEMOSTRACIÓN. Sea G un grupo. Consideremos G visto como conjunto (es decir en este caso $X = G$), y consideramos la aplicación

$$\begin{array}{ccc} X & \xrightarrow{Id_X} & G \\ x & \longmapsto & x \end{array}$$

Entonces, por el Teorema 7.1.9, existe un único homomorfismo

$$\varphi : F(X) \longrightarrow G$$

que hace conmutativo el siguiente diagrama



Es decir para todo $a \in X$ se tiene

$$\varphi \circ i_X(a) = Id_X(a) = a.$$

Por tanto φ es un epimorfismo, y aplicando el Primer Teorema de Isomorfía se tiene

$$F(X)/\ker(\varphi) \cong G.$$

■

Corolario 7.1.12 *Con la notación anterior, se verifica que* $F(X) \cong F(Y)$ *si y sólo si* card*(X)*=card*(Y)*.

DEMOSTRACIÓN. Basta aplicar el Corolario 7.1.10

■

7.2. Generadores y relaciones

Sea G un grupo, y sea X un conjunto tal que $F(X)/\ker(\varphi) \cong G$ mediante el homomorfismo φ definido en el Teorema 7.1.11.

Definición 7.2.1 *Con la notación anterior, a los elementos del conjunto* $\{\varphi(x) : x \in X\}$ *se les denomina sistema generador de* G. *Si* $\ker(\varphi)$ *es el mínimo subgrupo normal que contiene a* $\{w_i\}_{i\in\Lambda} \subseteq F(X)$, *decimos que* $\{w_i\}_{i\in\Lambda}$ *es un sistema de relaciones definitorias.*

Definición 7.2.2 *Una sucesión de grupos y homomorfismos*

$$\cdots \xrightarrow{f_i} G_{i-1} \xrightarrow{f_{i+1}} G_i \longrightarrow \cdots$$

se dice exacta en G_i *si* $Im(f_i) = \ker(f_{i+1})$. *La sucesión es exacta si es exacta en cada* G_i.

Definición 7.2.3 *(a) Sea* G *un grupo. Una presentación de* G *es una sucesión exacta de grupos*

$$1 \longrightarrow N \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1$$

con F *libre y* $N = \ker(\varphi)$.

(b) Diremos que N es la clausura normal de un conjunto $\{w_1, \ldots, w_n\} \subseteq F$ si N es la intersección de todos los subgrupos normales de F que contienen al conjunto $\{w_1, \ldots, w_r\}$.

Observación 7.2.4 *La clausura normal de un subconjunto de F es el mínimo subgrupo normal de F que contiene al subconjunto.*

Definición 7.2.5 *Diremos que:*

- *G es finitamente generado si admite una presentación*

$$1 \longrightarrow N \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1,$$

donde $F \cong F(X)$ con $\text{card}(X) < +\infty$.

- *G es finitamente presentado si se verifica:*
  1. *G es finitamente generado.*
  2. *N es la clausura normal de un conjunto $\{w_1, \ldots, w_n\} \subseteq F$.*

Notación 7.2.6 *Para un grupo G, su presentación será denotada*

$$G = \langle X | N \rangle.$$

Ejemplo 7.2.7 *Se tienen los siguientes ejemplos de grupos, dados por su presentación.*

1. *Un grupo abeliano libre G con base X tiene presentación*

$$G = \langle X | \ xyx^{-1}y^{-1} = 1, \text{ para todo } x, y \in X \rangle.$$

2. *Un grupo libre F con base X tiene presentación $F = \langle X | \emptyset \rangle$.*
3. *$\mathbb{Z}/4\mathbb{Z}$ tiene presentación $G = \langle x | \, x^4 = 1 \rangle$.*
4. *$G = \langle x, y | \, x^2y^{-3} = 1 \rangle$.*

Observamos que tiene sentido el recíproco: Dado X un conjunto no vacío, Y un conjunto de palabras reducidas en el alfabeto X, existe un grupo G con generadores X y relaciones Y. Para ello, se toma $F = F(X)$, y se considera la clausura normal N de Y en $F(X)$. Entonces $G = F/N$ satisface dicha propiedad. Es más

Teorema 7.2.8 (Teorema de Van Dyck) *Sea X un conjunto no vacío, Y un conjunto de palabras (reducidas) en el alfabeto X, y sea G el grupo definido con generadores X y relaciones Y. Si H es un grupo generado por X, y satisface $w = 1$ para todo $w \in Y$, entonces existe $\varphi : G \longrightarrow H$ sobreyectiva.*

DEMOSTRACIÓN. Por el Teorema 7.1.9, la aplicación $X \hookrightarrow H$ extiende a un epimorfismo

$$f : F(X) \longrightarrow H.$$

Como $w = 1$ para todo $w \in Y$, se tiene

$$Y \subseteq \ker(f),$$

donde $\ker(f)$ es un subgrupo normal de $F(X)$. Por tanto N, el subgrupo normal generado por Y en $F(X)$, está contenido en $\ker(f)$. Así se tiene que f induce un epimorfismo $F(X)/N \longrightarrow H$, es decir

$$G \cong F(X)/N \longrightarrow H$$

es un epimorfismo.

■

El problema que se plantea es el de identificar un grupo a partir de una presentación dada.

Ejemplo 7.2.9 *1. El grupo $\mathbb{Z}/6\mathbb{Z}$ tiene un generador x y una relación $x^6 = 1$, es decir*

$$\mathbb{Z}_6 = \langle x \,|\, x^6 = 1 \rangle.$$

Otra presentación del grupo $\mathbb{Z}_6$ viene dada por

$$\mathbb{Z}_6 = \langle x, y \,|\, x^3 = 1,\ y^2 = 1,\ xyx^{-1}y^{-1} = 1 \rangle.$$

2. El grupo de los cuaterniones tiene presentación

$$Q = \langle a, b \,|\, a^4 = 1, b^2 = a^2,\ bab^{-1} = a^{-1} \rangle$$

y

$$Q = \langle x, y \,|\, xyx = y,\ x^2 = y^2 \rangle.$$

Observemos que, en el primer ejemplo, se prueba que ambas presentaciones dan grupos isomorfos usando el Teorema de Van Dyck. Tomemos

$$G = \langle \alpha \,|\, \alpha^6 = 1 \rangle, \qquad H = \langle x, y \,|\, x^3 = 1,\ y^2 = 1,\ xyx^{-1}y^{-1} = 1 \rangle,$$

y definamos

$$F = F(\{\alpha\}), \qquad E = F(\{a, b\})$$

los grupos libres en 1 y 2 generadores respectivamente.

Si definimos morfismos

$$\begin{array}{ccccc} F & \xrightarrow{\varphi} & E & \xrightarrow{\pi} & H \\ \alpha & \longmapsto & ab & & \\ & & a & \longmapsto & x \\ & & b & \longmapsto & y, \end{array}$$

observemos que

$$\pi \circ \varphi(\alpha)^6 = (xy)^6 = x^6y^6 = (x^3)^2(y^2)^3 = 1.$$

Por tanto, $\alpha \in \ker(\pi \circ \varphi)$, y así $\pi \circ \varphi$ factoriza a una aplicación

$$\begin{array}{rcl} \psi : F/\ker(\pi \circ \varphi) & \longrightarrow & H \\ \overline{\alpha} & \longmapsto & xy. \end{array}$$

Como $xy = yx$ y $\text{mcd}\,(o(x), o(y)) = 1$, tenemos $o(xy) = 6$, de donde

$$\ker(\pi \circ \varphi) = \langle \alpha^6 \rangle.$$

Así, $F/\ker(\pi \circ \varphi) \cong G$. Obviamente, ψ es monomorfismo. Ahora si, H es finito, y $o(H) = 6$, habríamos acabado. En este caso sólo hay que enumerar los elementos de H:

$$1, x, xy, x^2, x^2y, y.$$

El problema es, en general, determinar si el grupo es finito, y cual es su cardinalidad. El hecho es que es un problema irresoluble, dada una presentación de un grupo, decidir cual es su orden. La razón es el siguiente resultado.

Teorema 7.2.10 (Novikov, Boone, Buitton) *Existe un grupo finitamente presentado $\mathcal{B}$ tal que no puede decidirse computacionalmente si una palabra arbitraria en los generadores de $\mathcal{B}$ es* 1.

Existen algoritmos ([8]), como la enumeración de conjuntos de clases, debido a Todd y Coxeter (1936), que permiten calcular el orden de un grupo para una presentación dada, supuesto que el algoritmo se detenga. Pero el Teorema 7.2.10 implica no sólo que es imposible saber a priori si esto sucederá, sino que garantiza que para cualquier algoritmo existe un grupo finitamente presentado que no puede ser tratado con ese algoritmo.

7.3. Ejercicios

1. Se pide:

   a) Convertid las siguientes palabras en el alfabeto $\{x, y, z\}$ en palabras reducidas:

- $w_1 = x^{-1}y^3y^{-1}z^{-2}zzy^{-1}z^{-4}z$.
- $w_2 = z^3y^{-2}xx^{-1}yx^4z^{-6}z^4$.
- $w_3 = zy^5y^{-2}y^{-3}z^5x^2z^{-1}zx^{-3}xz^{-4}x^{-4}y$.

b) Comprobad que $w_1w_2 = x^3z^{-2}$, $w_2w_3 = z^3$ y $w_1w_2w_3 = x^{-1}y$.

2. Demostrad que el grupo libre de rango 2 contiene un subgrupo libre de rango numerable.

3. Sea F un grupo libre sobre el conjunto X, y sea $F' = [F : F]$. Probad que F/F' es un grupo abeliano libre sobre el conjunto

$$\widetilde{X} = \{xF' : x \in X\}.$$

4. Sea F_n el grupo libre de rango n. Probad que F_n tiene un subgrupo de índice 2.

5. Sea F un grupo libre de rango mayor o igual que 2. Probad que existe un automorfismo de F de orden 2 que no deja fijo a ningún elemento de F diferente del neutro.

6. Sea F un grupo libre, y sea N el subgrupo generado por $\{x^n : x \in F\}$ con $n \in \mathbb{N}$ fijado. Probad que N es un subgrupo normal.

7. Sea $G = \langle a, b \mid a^8 = b^2a^4 = ab^{-1}ab\rangle$. Probad que $o(G) \leq 16$.

Bibliografía

[1] E. Bujalance, J.J. Etayo, J.M. Gamboa, *"Teoría Elemental de grupos "*, Cuadernos de la UNED, 1989.

[2] P.M. Cohn, *"Álgebra "*, vol.I. John Wiley and Sons. London, 1973.

[3] P. Dubreil, *"Teoría de grupos"*, Reverte, Barcelona, 1975.

[4] I.N. Herstein, *"Topics in Algebra"*, 2nd edition, John Wiley and Sons, London, 1975.

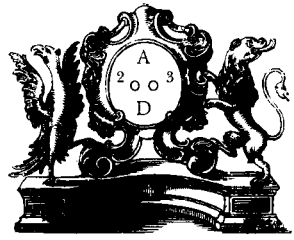
[5] T.W. Hungerford, *"Algebra"*, Graduate Text in Mathematics, **73**, Springer-Verlag, Berlin, 1974.

[6] S. Lang, *"Algebra"*, Aguilar. Madrid, 1971.

[7] E. Nart, *"Grups abelians finitament generats i formes quadràtiques"*, Publ.UAB, 1995.

[8] J.J. Rotman, *"An introduction to the Theory of Groups"*, Graduate Texts in Mathematics, **148**, 4th edition, Springer-Verlag, Berlin, 1994.

[9] A. del Río, J.J. Simón, A. del Valle, *Álgebra Básica*, Texto-Guía. Universidad de Murcia, 2001.



Este libro se terminó de imprimir el día 15 de febrero.
festividad de San Faustino y Santa Jovita,
hermanos, que predicaron
valientemente el cristianismo.

UCA Universidad de Cádiz

Servicio de Publicaciones
2003

ISBN 84-7786-807-7